计算机网络安全技术在网络安全维护中的应用

李　可
北京计算机技术及应用研究所　北京　100854

摘　要：计算机技术尽管具备便利性等优点，可是其安全性较低。在运行过程中，计算机网络安全也会受到黑客入侵、病毒入侵和安全漏洞等几种因素产生的影响，有可能出现数据丢失、系统异常等诸多问题。为了能维护计算机网络安全，应灵便运用互联网防火墙技术、入侵检测技术和加密网络安全技术等，降低其他因素对网络安全产生的影响。

关键词：网络安全；安全维护；安全技术；研究；计算机技术

引言：现阶段，各行业的发展都离不开计算机网络安全技术的大力支持。计算机网络安全技术的高效运用能够有效促进我国各行各业的发展趋势，能够更好地执行可持续发展战略。可是，计算机网络安全技术在国内的运用还存在一些急需解决不够。因而，文中对怎样正确运用计算机网络安全技术维护保养网络安全进行了详细科学研究，并对存在的问题给出了一些建设性意见，期待计算机网络安全技术能够获得灵活运用[1]。

1 计算机网络安全的基本概述

对于计算机网络安全的认识能够分为四个层面：（1）系统安全。这也是信息系统软件素材，都是系统优化的关键难题，包含硬件与软件机器设备。（2）网络信息安全。核心内容是采取有效措施保证数据信息免遭未授权的公布、伪造和破坏。（3）行为安全。它是以主体的过程与结果来考察它是否会严重影响与确保信息安全性的举动。（4）网络安全内容。换句话说，信息安全性在法律和道德方面的基本要求词义安全性。机器设备安全性主要体现在机器的易用性、可靠性和稳定性，别的三个方面一般是安全性、安全性和一致性。安全性，主要分硬件与软件安全隐患，例如信息机械故障、电脑操作系统系统漏洞、恶意程序威协这些。安全性，主要表现在数据信息不会被未经授权者所熟知的特性，应该是静态数据存储和动态性传送数据开展数据加密，是网络运维的关键方式。完好性，在违法行为的过程与结果中，保证数据信息正确、真实、没被变更的和完美[2]。

2 计算机网络安全技术的作用

在开展网络安全工作的时候，管理方案和相关应用的理论改善有重要使用价值。并对给与更多关注，能使信息系统软件具有更高的安全性和可靠性，保证系统的合理运转。在当代大数据技术高速发展的我国，网络安全导致了社会各界人士高度关注。不一样单位和个人对待与分析的方式方法和构思是不一样的。因而，消费者对网络安全的认识是不一样的，用户需要十分重视个人隐私安全。就企业来说，必须有效避免冒名、监听商业机密，提升信息安全防护，有效保障信息的完整性和安全性。除此之外，国家根据合理设置安全部，能有效抵挡外部的不法侵害。假如国家信息泄漏或遗失，将会对国家的物力和资金导致巨大损失，甚至导致社会混乱。因而，在现代社会的发展过程中，网络安全具备至关重要的使用价值。

3 目前网络安全维护中出现的问题

随着经济的进步和网络数据技术的不断发展，大家在实际生活与工作中越来越多的应用计算机网络，计算机网络发挥了越来越重要的作用，极大地提高了大家工作效率以及生活状态的效果。但是，根据互联网的关键技术大大增加，网络信息安全五花八门。因而，必须改善与创新信息安全技术，提升其在维护中的运用，进一步增强其安全性能。对于网络信息安全维护存在的问题，本文主要从以下几方面展开分析：

3.1 计算机病毒问题

电子计算机病毒具备高度感染性和毁灭性。一般来说，病毒包含不同种类，如木马病毒和特工病毒。其中，脚本制作病毒通常是利用网页页面脚本制作进一步散播病毒，将安全漏洞作为核心进攻目标，与此同时毁坏终端设备，从而深层管理程序[3]。木马病毒病毒是一种装出来的特定软件，它引诱客户免费下载与应用，毁坏其电子计算机，盗取客的信息内容，有时候能够完成对主机远程操作。恶意程序病毒进一步依靠首页与用户连接挟持其的信息内容，并充分利用强制执行措施吸引住大家进行浏览。伴随着信息内容技术的不断发展，出现大量类型的病毒，在很大程度上严重影响网络信息安全。

3.2 黑客攻击问题

在计算机网络维护中，黑客入侵对网络信息安全伤害主要体现在虚报连接信息及规模性总流量、病毒等网

络信息安全拒绝服务攻击，这也是目前计算机网络维护中常用的黑客入侵方法，即通过以上拒绝服务攻击，向电子计算机推送对应的专业软件或病毒连接，再将病毒嵌入电脑终端，这便是虚报连接信息内容拒绝服务攻击；使应用系统偏瘫的黑客入侵方式就是规模性流量式攻击；病毒进攻是由木马病毒或其它病毒操纵电子计算机，对计算机网络造成破坏的黑客入侵，对于计算机网络安全性维护有害危害十分突出。

3.3 网络本身的开放性会带来安全隐患

计算机网络的一个重要特征是其可扩展性和开放性，这在很大程度上严重影响计算机网络安全性。在其中互联网平台关键完成信息的传递和共享，联接行业非常普遍，信息的传递效率也十分高效率和精确。在计算机网络收集和传送信息内容的过程当中，难以绝对保证网络信息安全，并且由于节点数量众多，每一个接入网络的终端设备都会危及网络信息安全。一些犯罪分子利用这一系统漏洞谋私利，从网络上盗取信息内容，散播病毒。

3.4 操作失误问题

除了以上安全隐患，客户操作失误也会造成计算机网络安全隐患。例如用户在使用计算机时，错失了一些含有病毒的网站或连接，让犯罪分子趁虚而入，为电脑操作系统种下安全风险。此外，目前很多软件都要实名验证，用户将私人信息上传至不同类型的互联网平台很容易出现数据泄露。

4 网络安全维护中计算机网络安全技术的应用策略

4.1 网络入侵检测技术的应用

第一、网络入侵检测技术的概念。网络入侵检测技术又称为网络即时健康技术，它可以利用软硬件建设对网络系统实现实时监控系统。假如检测出攻击能力数据信息，将采取有效对策防止不良数据与信息的入侵。简单来说，网络入侵检测技术能有效阻拦故意入侵，确保电子计算机网络的安全性。网络入侵检测技术功能完善，能够监管与分析客户的活动，对体系结构和缺点开展全面审计，精确鉴别电子计算机网络里的攻击能力活动，对电子计算机网络全面的行为问题进行统计与分析。第二，网络入侵监测系统的种类。网络入侵监测系统主要包含两类，即系统软件已有监测系统和独立的网络入侵检测系统[4]。最先，系统软件自带的检测系统。电子计算机网络将自动运用检测技术全方位监测系统数据信息，从而增强信息安全性。系统软件带有的监测系统精确率较高，但也可能漏验。第二，单独的网络入侵监测系统。单独的网络入侵监测系统会收集和处理数据，分析判断进到系统安全性，假如数据信息有什么问题，会往日志见证者发出警告，便于其没有办法进入系统。第三，网络入侵检测技术的应用。有效运用网络入侵检测技术有益于保障计算机网络安全性。总而言之，网络入侵检测技术在计算机中网络安全性中的运用主要表现在下列四个方面。最先，网络入侵检测技术能够实时监控系统消费者和全面的各种各样活动，并且对消费者的操作行为和系统软件进行系统评定。次之，网络入侵检测技术能够全方位监控威协个人行为，记录威协个人行为的实际全过程。另外，网络入侵检测技术能够全方位统计分析电子计算机网络里的行为问题。最后，网络入侵检测技术能够追踪操作系统的财务审计，判定客户是不是有所影响网络安全个人行为，并通过分布式系统入侵检验、智能化入侵检验与安全入侵检验开展阻拦，维护客户的个人权益。

4.2 防火墙技术的应用

最先，运用网络信息安全配置。在防火墙技术中，网络信息安全配置是很重要的，它可以有效的将系统软件划分成块，防护最主要的保护控制模块进行安全保护。此外，对于这些隔离地区，在防火墙技术的作用下，可以和外网地址防护，从而形成一个局域网络，依然可以根据自身内容做出管理决策，做出有效指示。不会受到外界网络的作用和影响，进一步提高了系统稳定性和安全性。二是方法与对策的应用。针对网络防火墙而言，一个关键性的一部分就是可以适用互联网安全防护活动合理开展的访问策略。根据对互联网的科学配置和科学安排，可以进一步优化系统信息的统计步骤，搭建相对性完备的保护管理体系。与此同时，防火墙技术也可以根据当前网络工作状态科学整体规划访问策略，持续改善网络空间，进一步提高系统软件使用效率[5]。三是日志监控的运用。在实际的电子计算机保护运行和开发环节中，保护日志起着非常重要的作用与价值，它能够纪录用户系统的所有主动与被动网络活动，给予更有意义的信息。因而，科学可以用防火墙技术来监测和保护日志。一般，使用该方法的过程当中，大家可以打开网络防火墙登陆系统安全性。主要是因为工作范畴比较广泛，总体工作强度大。因而，依靠该方法，能够对信息资源搜集全过程进行合理归类，以达到纪录监控的性能和目地。与此同时，用户可以通过为信息目标选择相应的类型来获取信息，进而充足提升系统的结构和配置。

4.3 病毒查杀技术的应用

伴随着互联网技术的革新，电子计算机自然环境中

出现的病毒种类变得更多，其危害性会相对比较强。广为流传的“勒索病毒”根据数据加密目标受众的机器、本地文件和程序来敲诈勒索目标受众资源，这给受到攻击的消费者造成了巨大的资源损失。现阶段开发出来的病毒查杀技术大致可以分为主动与被动两种模式。在互联网维护保养环节中，维护员对病毒运作模式和目的开展逆向分析，不断创新完整的病毒包对电脑开展扫描仪查杀病毒。积极查杀病毒的关键在于选用动态防御技术，依据系统软件防御力要求，结合当前病毒关联性，开发出来的病毒防御专用工具可以在一定程度上提升互联网环境中的安全指数。

4.4 计算机加密技术与访问权限技术的应用

在互联网的运行管理中，因其互联网设备运行状态多为动态性方式存放，所以需要应用计算机数据加密技术和访问限制技术，防止数据和信息在系统运行里被盗取或伪造。在其中，电子计算机数据加密技术在网络运维中的运用就是把初始信息数据转化成登陆密码数据信息，根据正确密匙转变成最原始的文档格式，充分保证互联网运行时文件存储的安全性和完好性。除此之外，目前，我国所使用的数据加密技术在互联网维护保养主要包含对称加密算法和对称加密。前一种数据加密维护方式在加密和解密中都可以用，后一种加密方法在加密和解密时密匙具体内容不一样。面对这种情况，在计算机中数据加密安全性技术的应用中，应根据实际情况，从以上二种数据加密技术的实际特性考虑，开展合理的选择与应用，以适应互联网维护保养的安全性和性能要求。除开电子计算机数据加密技术，网络运维也可以通过电子计算机访问限制技术的应用，在数据库访问环节中设定对应的管理权限或难题，键入标准答案或授权之后才能浏览有关数据和信息，充分保证互联网的网络信息安全，减少互联网运行时被黑客入侵或病毒感染的风险[6]。

5 增强计算机网络安全性的管理策略

要进一步维护保养计算机网络安全性，既需要灵便运用计算机网络安全生产技术，还要做好相对应的管理工作，完善管理体系，为计算机网络安全生产技术的有效运用打下基础。最先，管理者必须结合实际情况制订计算机网络安全管理规定，确立计算机网络的操作方法和程序，降低人为因素带来的影响。次之，管理者必须升级、更新与维护计算机网络。计算机网络系统及专业软件是不断创新和优化的，管理者要不断更新系统软件，按时用电脑杀毒软件等设备检查设备[7]。除此之外，管理者要加强对计算机网络的监管。计算机网络尽管有极强的便捷性，但也有一定的开放性与虚构性，因此计算机网络转变迅速。仅有做好对计算机网络的监管，才可以充分运用计算机网络安全生产技术的功效。因而，管理者必须通过合理的方法对计算机网络全面的安全隐患展开调查，从而减少安全隐患对网络安全的危害性，保证应用系统的安全运作。

结束语：总而言之，网络安全一直是社会发展关注的重点。计算机功能系统在使用中很容易受到病毒和网络黑客攻击，出现一系列网络安全难题，为人们的生活和工作带来很多不便。因而，为了保障计算机网络安全性，必须加强这一块的关键技术研究，联系实际难题，规范使用网络安全技术，如入侵检测技术、防火墙技术和加密技术，维护应用系统里的网络信息安全，为客户提供更好的上网自然环境。

参考文献

[1]许晓璐.计算机网络安全技术在网络维护中的应用[J].电脑编程技巧与维护,2021(2):159-160+173.

[2]孟大淼.计算机网络安全存储中云计算技术的应用[J].电子技术与软件工程,2021(15):243-244.

[3]田扬畅.计算机网络安全防范技术的研究和应用[J].普洱学院学报,2021,37(6):31-33.

[4]吴家存.试谈大数据时代的计算机网络安全及防范措施[J].网络安全技术与应用,2022(4):71-72.

[5]顾雷鸣.计算机网络安全技术在网络安全维护中的应用探讨[J].计算机产品与流通,2020(06):71.

[6]姜可.基于网络安全维护的计算机网络安全技术应用分析[J].计算机产品与流通,2020(05):42.

[7]沈伟.计算机网络安全技术在网络安全维护中的应用[J].信息与电脑(理论版),2021(21):203-204.