基于网络安全维护的计算机网络安全技术

沙牙古力·巴依毛拉
塔城职业技术学院　新疆　塔城　834700

摘　要：随着信息化时代的到来，使得计算机网络技术在各个行业和领域当中都得到了越来越广泛的应用，并且发挥出了越来越重要的作用。可以在极大程度上彻底改变了我们以往传统的工作与生活模式，为我们提供了巨大的生活方便。在如此的趋势下，社会各界对于安全工作更加关注。就目前的状况分析，当前互联网实际使用的过程中，也面临着很多的安全隐患，一旦无法对其做出合理的预防和处理，将给社会带来非常巨大的冲击和风险，给人们的工作和生活造成极大的不便。

关键词：网络安全维护；计算机；网络安全技术

引言：在如今的社会环境中，计算机网络科技给我们的日常生活带来了诸多的方便，很大程度上彻底改变了我们原来的日常生活模式，大量过去较为繁琐的日常信息都能够借助互联网加以解决。然而在人类如此依靠互联网的当下，安全问题却也是日益严重，大量安全领域的案例正在不断提醒着我们对人类互联网安全的重视，而我们的个人信息和隐私权也在当下的互联网世界中正在受到着巨大的影响。因此，完善当前的计算机网络技术，从而改变当下的安全无法保证的局面，这是当今十分关键的任务。

1 网络安全维护概述

网络安全维护是确保网络环境持续稳定运行、有效保护用户数据免受非法获取与篡改、以及严密防范来自各方的各种潜在网络攻击与威胁的关键过程，对于维护网络秩序、保障信息安全具有重要意义。信息技术的飞速发展和普及，网络已成为现代社会不可或缺的基础设施，无论是个人日常生活的便捷沟通、娱乐学习，还是企业运营的顺畅进行、数据管理，乃至国家管理的高效实施，都高度依赖于网络环境的稳定与安全。网络安全维护的核心目标是防御外部威胁，如黑客攻击、病毒传播、恶意软件入侵等，同时确保内部数据不被非法访问或泄露。这要求对网络系统进行全面的安全评估，识别潜在的安全漏洞，并采取相应的防护措施。这些措施包括但不限于安装防火墙、部署入侵检测系统、加密敏感数据、定期更新软件补丁等。网络安全维护还需关注用户行为管理，通过教育用户识别网络钓鱼、诈骗等常见网络威胁，提高用户的安全意识，减少因人为疏忽导致的安全事件[1]。建立严格的访问控制机制，确保只有授权用户才能访问敏感资源，进一步降低安全风险。在应对网络攻击时，网络安全维护团队需具备快速响应和恢复的能力，一旦发生安全事件，应立即启动应急预案，隔离受影响的系统，防止攻击扩散，并尽快恢复网络服务的正常运行。同时，对事件进行深入分析，总结经验教训，优化现有的安全防护措施。网络安全维护是一个持续不断的过程，需要综合运用技术、管理和法律等多种手段，随着网络环境的不断变化和新型威胁的不断涌现，网络安全维护的策略和方法也需不断更新和完善。只有这样，我们才能确保网络环境的安全稳定，有效抵御各种网络风险与挑战，从而为社会的信息化发展提供坚实可靠的保障，推动数字经济的繁荣发展。

2 影响网络安全的因素分析

2.1 计算机系统的安全性不高

计算机一旦不符合较高的安全系数，就很容易出现网络安全问题。每台电脑的操作系统都必须进行自动更新，不然就很容易发生安全漏洞，有的病毒和木马就可以由此进入，从而给上网系统的安全和稳定性造成了威胁。另外，使用者在浏览一些不当的网站后也可能会导致个人信息的流失。所以需要做好对计算机系统的更新和修改工作，以提高操作系统的安全性。不过操作系统并没有总是绝对安全的，因为往往有人会利用系统漏洞而进入到计算机系统里面，对计算机的安全性产生了影响。

2.2 黑客对计算机的攻击

由于计算机的实力日益提高，黑客们可以利用在电脑上潜伏的病毒对整个计算机实施控制。许多客户在使用电脑的过程中，通常都不会配置杀毒软件，所以单纯的安装防火墙并不能对抗骇客的进攻。不过，骇客也能够透过查看攻击者计算机中的安全漏洞来获取信息，甚至可以对存储和数据传输中的数据加以截取，导致内部数据直接上的损坏，严重的甚至可能造成网站崩溃。通常情形下，电脑在受到入侵后的极短时间内往往难以确

定攻击原因，再加上黑客们已经掌握了丰富的计算机应用技术以及超强的互联网操作能力，这也就导致在网民的安全上面临了一个更为严重的难题，所以网民们就必须要不断提高电脑的安全等级。

2.3 计算机的安全性能较低

计算机网络安全性能较低，则会容易出现安全性的问题。每一台计算机都应在最短的时间之内更新计算机系统，一旦出现相关网络安全的问题，病毒入侵其中，对于计算机的正常运行以及计算机网络的安全性有着一定的影响。与此同时，用户在浏览一些网站时极其容易出现泄露信息的问题，所以需要及时更新和升级计算机系统，不断提升信息网络的安全性能。但是并非所有最新的计算机系统都是安全的，一些不法分子趁着漏洞侵入到计算机系统的内部收集相关信息，导致用户的个人信息泄露，同时还会影响用户的计算机使用体验感。

2.4 软件造成的安全隐患

因此实现硬件工程，必须是用计算机软件为载体。许多不法分子利用制造的恶意软件来侵入并让用户上网，其中木马、病毒、流氓软件等，均具有传染性、强制性、复杂性、破坏性等特征，严重损害计算机的安全性。该木马病毒能够利用互联网作为传播介质，并针对计算机、硬盘、软件等作为病毒传播媒介，轻则干扰计算机的工作效率，重则盗用、侵犯他人信息，或者是盗取用户的上网资产[2]。计算机网络中毒的主要症状是:计算机上反映的速度慢、程序卡顿、连网速慢等问题。而通过传播木马病毒的主要目的，则是:窃取网络秘密、窃取个人财产、进行远程控制、损坏系统、盗取个人数据等，对使用者造成了很大的危害。

3 有效提升网络安全维护水平的计算机网络安全技术

3.1 防火墙网络技术

防火墙等网络技术在计算机信息网络安全中的应用，已经达到了相当完善的发展阶段。建立防火墙是实施互联网防护的重要措施，它能够有效防止计算机网络受到侵犯。在防火墙一般用来限制的范围内，对无法访问的IP实施阻挡，可以有效防止对不安全的IP以及软件的侵入和攻击。它们通过安全策略拦截了特定的网络流量，同时布章一般是自己安装的，可以自行修补其安全漏洞。总的来说，防火墙是保护计算机安全、避免计算机故障的安全屏障，而同时它又是人们必须采取的最基本维护计算法的保护措施。防火墙既可能是硬件、软件，也可以是二个或多台计算机之间的防火墙，它们在保护计算机领域上都开展了相应的实质性措施。而面对日益发展且难以预测的传统计算机病毒，相关机构人员也针对此类病毒的主要属性、特点、影响程度等方面都加以了仔细分析研究，并以此为基础从根本上有效防止了这些计算机病毒窃取用户计算机资料活动的进行，全面加强计算机网络病毒的安全预防管理工作。总而言之，在当前大信息时代背景下，加强防火墙的技术对中国的信息安全具有相当程度的重要意义。

3.2 数据加密技术

灵活利用数据加密技术进行安全保护的操作方式，即通过数据加密系统对大数据网络软件与信息系统的数据加以保护，并将明文信息数据转变成密文，在查阅过程中，如需恢复密文，则必须采用相关加密，尽可能减少网络数据的泄密风险。在互联网数据应用和信息传输工作中，应当增加信息数据加密技术的频次，对信息系统结构加以完善，增强数据稳定性，提供高质量信息传播环境。对网络的安全技术实际状况加以细致理解，对网络安全的加密技术也加以细分，比如我们可以将它分类为数据存储的加密技术、数据传输加密技术、内容识别加密技术等，并针对各种信息传输技术进行了针对性服务。在进行数据加密操作时，要坚持多元化原理，即对各种数据应用进行各种帮助，增强的数据稳定性，包括美国NewDES技术、欧洲IDEA技术的最超前技术。此外，数据加密技术也是安全产品体系主要部分之一，利用此技术能够有效减少非法入侵问题出现的可能性，有助于减少病毒入侵几率。将其与加密算法进行比较后认为，数据加密技术稳定性较好，能够协助管理人员有效进行安全保障操作。不过在实际使用中，数据加密技术还具有一些不足之处，所以工作人员将进一步对其完善，使得数据加密技术能够在安全保障事业上实现其最大作用。

3.3 网络身份安全验证技术的有效应用

由于网络的日益发达，目前它在我们的日常生活中的使用也变成了一个常态，在加上网络的安全性也进行了有效的改善与提高，许多个人电脑使用者就忽略了安全的重要性，部分电脑用户因为在个人电脑和互联网共同使用的环境中都没有和服务器进行过相互认证，因此从服务器上不能获取更多的用户资料，这也就让了服务器上对于电脑用户的一些安全数据不能充分了解，这在一定程度上也就增大了服务器安全问题出现的可能性。为使上述的难题得以合理解决，计算机用户也要结合实际情况将网络身份验证功能应用到物联网中，这样才能给用户网络上的安全带来必要的保护。目前计算机安全技术的应用也在日趋完善，尽管计算机用户身份验证功能也在网络的进程中得到了很有效的利用，但是，计算

机用户在浏览网络的进程中仍然很容易遭遇病毒的攻击，因为这种病毒大多是通过把软件功能与不良网络信息绑定在一起传播的，因此严重干扰了计算机用户对互联网的正常应用，不仅让计算机使用者的证件也不能有效的认证，同时，还会导致用户的个人信息泄密。面对上述情况，政府管理人员必须要格外注意安全与备案方面的重点工作，在服务器与计算机用户之间就建立起了双重的验证机制，并对其进行了不断完善和优化，从而于在一定程度上保证了计算机用户的安全。

3.4 网络入侵监测

现阶段威胁用户计算机安全的二个手段，一种是潜伏在系统的电脑上，等待指令对系统实施入侵，而另一个则利用网络直接侵入系统内。关于第一种入侵手段的防范方式，通常都是指通过对系统本地文件信息的检查，确定用户电脑自身中是不是存在有高风险的文件信息，并由此来对系统内的病毒信息加以查杀。不过，在这一方面由于用户计算机本身的使用局限性，也可能出现了一些检测错误的现象，因此检测结果也就比较有限。而针对第二种攻击方式的防御，可以实时监控用户的网站浏览状况，对客户的浏览情况做出即时的监测，评估客户的电脑是不是在使用过程中遭到外来电脑的访问，通过评估结果给客户进行安全方面的建议，以避免一些安全性风险[3]。这一方法能够避免大部分的外部非正常访问问题，不过由于客户端自身计算机的权限问题，那些利用互联网异常传递的信息仍然不能正常地被这一防范手段所监测到，还是会产生相应的安全问题。因此，它要求计算机网络防御技术在侦测异常的同时，还需要通过一些文件对计算机中数据的方位状态加以检测，检测的关键还在于这些软件有没有不断查询我们的历史数据和计算机系统配置，并通过长期的测试数据，来判断一些潜伏得很深的病毒攻击，从而来提高安全体系的防御能力。

3.5 提高操作人员使用水平

随着当前计算机技术的高速发展，电脑使用人员的逐步增多，而电脑使用人员的情况也直接决定计算机安全程度，所以要想提升计算机的安全就需要提升操作人员使用能力，让其具备相应的意识，在运行中对计算机加以维护。首先，应该进行安全教育工作，加强安全培训工作，以此增强大家对电脑的应用意识，使电脑应用人士可以在平时使用中对自己言行加以控制，减少网络安全问题发生的可能性。此外，还必须进行一定的安全技术培训与推广工作，使电脑应用爱好者能够认识电脑安全的意义，对其上网风险进行广泛探讨并引起一定注意，增强电脑应用的意识和自身保护，有助于对基础上网问题做出判断和进行解决工作。最后，在计算机应用人进行日常应用的过程中也需要经常进行密码操作，特别是对计算机主机以及与计算机直接连接的应用软件、装置等，都需要进行相应的密码操作，对于设定密码口令，还必须注意在进行密码口令设定时其口令信息不要过分简化，而要尽可能复杂并且定时做好调整动作，或者根据其真实情况对其信息进行定时更改，同时相关应用人还需要做好密码保护操作，以保证信息的安全与准确性。

结语

总之，在计算机等网络科技日益发达的大背景下，使用者们所面对的互联网环境也在不断的产生着改变，使用者的网络也面临着巨大的安全隐患。为避免这些现象，应注意网络安全保障工作的必要性，对网络设备进行测试，以充分发挥现代互联网信息技术的优越性，以确保计算机网络设备在正常工作流程中的安全性与可靠性，并进一步增强安全保障的有效性，从而给使用者营造一个健康安全的上网环境，促进计算机网络系统在人们生产和生活中发挥出最大的价值。

参考文献

[1]王瑞梁.基于网络安全维护的计算机网络安全技术应用分析[J].电脑知识与技术，2021，17(09):56-57.

[2]王辉鹏.基于网络安全维护的计算机网络安全技术应用分析[J].信息与电脑(理论版)，2020，32(19):190-191.

[3]高丽.基于网络安全维护的计算机网络安全技术运用[J].信息与电脑(理论版)，2020，32(18):199-201.