基于网络安全维护的计算机网络安全技术应用

周　波
河南省南阳市宛西中等专业学校　河南　南阳　473000

摘　要：随着科学技术的快速发展，计算机网络技术得到了明显的发展，并逐渐深入到社会发展的各个领域，给人们的生活创造了良好的条件。但是，一些计算机网络安全问题接踵而至，严重影响着人们对计算机的正常使用。基于此，本文分析了影响计算机网络安全的因素，并给出了计算机网络安全维护技术的应用策略，希望能够为相关研究提供借鉴。

关键词：网络安全维护；计算机网络；网络安全技术

引言

计算机网络中存在的安全隐患严重困扰着计算机用户，为了能够给计算机用户创设一个安全健康良好的网络环境，需要明确影响网络安全的相关因素，并利用先进的计算机网络安全技术对网络进行不断完善和优化，解决传统网络中存在的安全问题，切实保障网络安全稳定运行，为人们日常生产生活活动的顺利有效开展奠定良好的基础。

1 影响计算机网络安全的因素

1.1 黑客攻击

黑客攻击是计算机网络运行遭遇安全威胁，引起计算机存储信息泄密、内部文件遭破坏、传输信息遭拦截等安全问题的重要原因之一。根据黑客攻击的破坏性情况，可以将计算机网络安全攻击分为非破坏性攻击和破坏性攻击。其中，非破坏性攻击行为的目的在于扰乱计算机系统的运行，通常采用拒绝服务攻击或者信息炸弹等手段；破坏性攻击是以窃取系统中的信息、破坏目标系统数据等为目的。

1.2 计算机网络自身问题

针对计算机来讲，其在必要开发网络环境中，能够将自身的功能与作用全面发挥，从而为人们带来更多帮助，所以在各类软件应用的过程中，由于不法分子会在软件内植入病毒，这会严重影响系统的正常运行，甚至较为严重的会导致系统漏洞百出，很大程度上对计算机用户，对信息安全造成了较为严重的威胁，而且由于现阶段系统开发的速度相对较快，从而导致无法精准地对一些病毒进行识别与处理，这会严重影响计算机网络自身的安全性，从而因自身的因素影响受到较为严重的限制，不法分子会通过计算机自身的漏洞，获取相关资料信息或恶意篡改计算机网络内部信息对用户的信息安全造成一定的影响[1]。

通讯作者：周波，出生于1984年08月，汉族，男，籍贯：河南南阳，单位：河南省南阳市宛西中等专业学校，职位：招生办副主任，职称：讲师，本科学历，邮箱：wxzzzb@163.com，邮编:474350，研究方向：计算机

1.3 病毒的攻击

针对网络病毒来讲，通常是由不法分子所导致企业会根据自身的技术，在某些软件中植入病毒，其为了能够谋取利益，对病毒会进行不断的优化，黑客将病毒植入到计算机系统，并潜伏在计算机系统之中，在需要获取一定利益的时候，则会发出指令，则会对计算机的系统进行破坏与影响，而且目前比较常见的病毒大多是捆绑性质的脚本或木马，大部分病毒都会有蠕虫类病毒的传播性与潜伏性，一旦没有得到及时处理，则会长期窃取有关信息，从而影响用户信息的安全性。

2 提高计算机网络安全性的技术策略

2.1 规范使用计算机网络入侵检测技术

网络入侵检测技术是检测网络安全威胁的重要技术手段，对于扫除网络安全隐患，营造安全、可靠的网络空间有积极的作用。在使用计算机系统开展活动时，用户要科学选择和使用计算机系统自带的入侵检测技术功能，定期对计算机系统的安全性进行检测，并根据检测结果进行相应的修复操作，确保潜在的计算机网络安全漏洞能够被及时发现和解决。需要注意的是，计算机网络入侵检测是计算机系统自带的检测功能，需要用户定期对检测技术进行更新、升级，避免检测技术自身存在较大的安全漏洞，威胁计算机系统的安全[2]。

2.2 数据加密与访问权限技术

针对现阶段我国网络安全易出现的问题，笔者将展开介绍以下几种安全防护措施，首先在数据的加密方面，用户个人信息、数据具有强烈的隐私属性，所以为

数据加密的安全技术在网络安全防护方面具有十分关键的重要作用。其中，密钥技术对于数据、信息的保护效果十分明显。这种安全防护技术的使用范围非常广泛而且成本较低，在全国范围内的许多领域的设备系统中都有密钥技术做基础安全防护。其次，访问权限技术也是有效提升计算机系统安全性的方法。访问权限一般指，只有拥有授权的用户才能进行系统访问，最大限度地杜绝了外来人员的非法访问。例如：在某公司内部网络分为两部分，一部分是外来人员可以随意访问的共用网络，其次是公司内部的局域网络，且局域网络无法与共用网络相连，保证了公司重要数据和信息等文件的传输安全性与隐私性。

2.3 先进信息加密技术的有效应用

一般用户的私密文件和相关的数据信息是黑客和计算机病毒入侵的主要对象。为了有效保护用户私密文件和数据信息不被盗取，需要加大对网络安全信息加密技术的应用力度，用户可以将验证技术和加密技术结合起来使用，这样可以有效提升验证的效果，避免用户的信息被恶意盗取。因为计算机网络在登录过程中都需要登录账号，用户想要使用计算机就必须将自己之前设定的账号和密码准确输入，这样才能拥有对计算机网络的使用权。在此过程中，要给输入密码的安全性提供有效的保障，用户还可以根据具体的情况采用先进的加密技术对密码加密。当然相关工作人员要加大对加密技术的研发力度，对各环节检测工作有效落实，同时综合多种加密技术的优势。保障信息数据在传输的过程中的安全性和稳定性，以免其在传输过程中受到相关外界因素的影响而出现信息泄露让计算机用户遭受一定的损失。此外，在加密节点的过程中，工作人员要采用密码装置来处理信息的节点，并在节点连接对相关数据获取的过程中采用先进的加密技术对数据加密，提高获取数据的准确性，从而保障用户上网环境的安全性，有效提高加密技术在应用过程中的安全等级。为了全面保障数据在传输过程中的安全性和准确性，工作人员还可以采用加密技术针对数据在传输过程中的任何一个节点设计相关的加密程序，不断提高数据的安全等级，为后期工作的顺利有效开展提供有效的数据参考[3]。

2.4 科学选择使用商业化的网络入侵检测系统

与计算机系统自带的网络入侵检测技术不同，商业化的网络入侵检测系统是由专门的计算机网络安全主体根据计算机网络威胁开发的综合性检测技术方式，可以定期对计算机系统中的网络隐患进行排查和修复，并提醒用户在使用计算机系统时需要注意的网络安全问题。为确保计算机网络的安全，用户要根据自身的需求选择和使用相应的商业化计算机网络入侵检测设备或者软件，以提高计算机系统的安全性和可靠性。

2.5 系统备份以及还原技术

计算机系统中通常具有系统备份以及系统还原两种十分便捷的基础功能，但这需要用户在平时的使用中就注意将自己的数据、信息习惯性地备份，否则在进行还原过程中易造成数据丢失。在系统遭受了核心代码的篡改或缺失后，整个计算机是无法继续运行和工作的，系统还原功能能够使计算机恢复到正常运行阶段的任何节点中，非常方便。对于用户数量基数庞大的企业级运行系统而言，备份与还原技术能够为用户信息的安全提供优良保障。

2.6 提高网络用户的安全意识

计算机运行安全问题不仅受软件硬件的影响而且与用户的安全意识有着密不可分的关系，因此为了避免受多种因素影响，从而保证计算机安全稳定的运行，则需要不断提高计算机用户的安全意识，这样能够确保其根据实际情况合理的运用计算机，从而适当的下载安全防护软件，这样能够保证计算机稳定运行，不存在违规网站设置下载软件，使得计算机运行效率大幅度提升，保证其运行的安全性，避免受不良因素影响而导致计算机内部网络及信息被窃取，只有这样才可以全面提高计算机网络安全防护的效果，为用户提供更多便捷的服务，弥补传统网络安全管理存在的问题[4]。

2.7 科学设置访问权限

访问权限的设置可以帮助用户将那些没有必要访问计算机系统的用户阻挡在外，从而避免网络访问行为可能产生的病毒传播现象。在使用计算机系统时，用户要合理设置相应访问密码等身份验证信息，并在系统中设置相应的身份识别、反馈内容，以提高计算机系统自身的访问安全性能。同时，计算机网络管理员应以IP为目标或以注册的用户名为目标，限制非法用户的网络访问权限，并对在线用户的网络访问情况进行监控，确保网络访问的安全、规范。

结束语：

营造安全、绿色、生态、健康的网络空间环境，是计算机网络安全技术有效应用的前提和基础。在计算机使用过程中，应持续并不断关注网络安全问题，了解网络安全隐患的发生机制，并采取相应的技术和管理手段来阻止各类安全隐患对计算机网络的破坏，保障计算机

系统运行的安全性、稳定性。

参考文献：

[1]童瀛.计算机网络信息安全威胁及数据加密技术探究[J].网络安全技术与应用，2021（4）：20-21.

[2]黄蓉.计算机网络安全与数据完整性技术探究[J].网络安全技术与应用，2021（4）：57-58.

[3]魏清刚.计算机网络安全技术在网络安全维护中的应用[J].网络安全技术与应用，2020（12）：3-5.

[4]杨婷.计算机网络安全中的防火墙技术应用分析[J].数字技术与应用,2020,38(5):177,179.