计算机网络安全技术的影响因素与防范措施

井 轩 瞿 源
汉江水利水电（集团）有限责任公司网络信息中心 湖北 武汉 430040

摘 要：随着时间的进展，互联网科技的发展速度也在日益提高，软件工程的逐步提高使得人类生存和工作的智能程度获得了提高。在实际使用计算机网络系统的过程中，通常都会遭遇一些网络安全因素的干扰，这也就很容易使计算机等网络设备面临安全危机，所以计算机网络系统的安全性问题也引起了我们的重视。

关键词：网络安全技术；影响因素；防范策略

引言：近些年来，我国在网络上的发展，不但在人们的日常生活中有所体现，在领域的研究中也逐步实现了渗透，为中国的经济社会发展和社会进步提供有力的保障。同时，为了加强对网络安全技术领域的研发，以及如何推动我国网络安全的现代化建设，也已逐步发展成为各个方面的重大研究课题，所以，构造出更加完备的计算机网络安全平台，就必须从网络安全平台中进一步完善并制订出针对性的技术防范措施，以维护国家网络安全生态的稳定。

1 计算机网络安全技术基本概况

计算机网络安全技术，主要是指通过采取特定措施来改造计算机硬件和软件，以及通过提高对其进行计算机信息数据处理时所具备的能力，使其减少遭受或甚至减少因为各种不同因素所带来负面的影响。现代网络安全的主要特征涵盖了安全，保密性，完整性以及可用性。其中的安全性特点，是说:对互联网信息在合法要求的前提下，实现所要求信息功能的特性。这也是互联网的要求最高和基本的特点之一。保密性特点是用来避免个人信息泄漏，从而产生一些不良影响的特性，这种特点主要是保障个人信息不被非权限的用户浏览。而完整性特点是保障网络上个人信息不被非法修改的特点，要求数据在制作，贮存，传递的过程中不会被更改，被盗，损失等，保证资料的原始数据的完整性。可用性是指数据能够获得客户许可和安全使用的特性，能够向授权客户提供服务，主要从使用期限和服务费用二种角度来评价[1]。在现阶段，随着互联网信息技术发展的深入，计算机网络应用范围越来越广泛，因此也就需要对其安全手段的大力推广与运用，使整个网络的应用环境更加完备、合理，从而形成了一种正向健康发展的新形势。不过，互联网安全本身就有一定问题和缺陷，在现实运用当中也存在着一定危害因素，面对这一问题就必须采取相应的预防措施，进而才可以使其顺利地运转，使之可以给整个计算机与网络信息技术的使用带来安全保护。

2 计算机网络安全技术的影响因素分析

2.1 信息数据的安全问题

由于云平台作为一种开放式的网络平台，部分消费者对平台用户名、口令的意识不足，极易被某些不法分子掌握，造成网络个人信息遭到泄漏。而在对互联网数据的管理中，信息通常采取的是二进制的方法加以保存，一旦数据库系统的管理技术出现泄漏之时，骇客就可以利用网络的脆弱之处对互联网实施入侵，窃取数据库的数据，甚至攻击操作系统的数据，由此导致大量互联网信息的流失，严重影响了用户对互联网数据的有效利用[2]。这就必须做好对互联网信息系统的安全管理，首先做好对互联网信息系统数据的安全保护工作，在互联网中设置了保护墙、杀毒软件等对互联网数据加以防护措施，就可以有效避免数据信息安全遭到泄漏、篡改、损毁的情形。

2.2 计算机系统存在漏洞

在对计算机的安全问题的探究过程中，人们可以看到，操作系统所带来的负面影响也是不容忽视的。它属于互联网运行、信息传播的一个重要基础，技术的革新起到了十分关键的作用。任何事物都会存在着被新事物所替代的机会，在整个计算机行业发展过程中也是这样，所以，电脑的操作系统必须创新，并在此期间通常也会补齐某些短板和缺陷。一旦电脑上发生了系统漏洞，就必然要为病毒入侵、骇客袭击等事件创造了条件，因此若要保障用户的安全使用，为了保证计算机的正常高效运转，就必然在第一时间修补操作系统上出现的缺陷和问题[3]。

2.3 用户安全意识淡薄

随着当前科学技术水平的日益提高，数字化社会的来临，现代人的娱乐与工作越来越远离互联网。不过，

一般来说网络本身并不能保证互联网的功能，同时使用者对互联网功能又缺乏很深刻的认识，再加上自己的安全意识不足，也容易使得互联网存在很大的安全危险。但是，很多互联网运营人员及其客户单纯的关注应用数据，忽略互联网数据的安全，很多网络使用者的心里也有着一定的侥幸心理，以为数据被盗或者黑客攻击的现象不会出现在自己身边，这就导致计算机互联网技术的作用没有得以发挥，给不法分子带来了可乘之机。

2.4 黑客与网络病毒攻击

站在互联网黑客的视角加以研究，其工作目的在于利用计算机网络体系中存在的漏洞等进行非法攻击或入侵，利用一个指定程序的网络进程对用户电脑进行控制，甚至窃取他们的一些信息和给予损害等。这种利用人类特征编写的网络程式具有很强的拷贝特性，能够在瞬间产生大量拷贝，从而会直接损害计算机网络系统的稳定性和安全[4]。针对存在的安全隐患的病毒种类来说，这些病毒具有强烈的适应性、攻击性等，在其入侵时一般无法对入侵范围予以识别，因此，当存在安全隐患的同时必然会给计算机系统的安全性和稳定性造成很大损害，由此可能造成一些内部档案、资料等流失、损毁甚至泄漏。比如有些大公司的许多商业秘密直接关系到企业的运作和经营，一旦不小心泄漏或是受损，则可能会被竞争对手所使用，进而造成一些重大损害。

2.5 外部环境问题

尽管计算机上配备当前较为领先的硬件设施和应用软件设备，但还是无法确保计算机的安全性。在这些情形下，外部网络安全环境则成为了入侵计算机系统的重点目标，对计算机安全运营造成了一定的危险。所谓的外部互联网环境，通常就是指互联网黑客[5]。这些不法分子为谋求更多的个人利益，往往不择手段，通过对目标计算机系统的程序数据实施频繁入侵，以从中查找出目标计算机系统本身所存在的技术漏洞，并以此为切入点，对目标计算机所处的网络安全环境进行攻击，以此实现窃取信息数据并摧毁目标计算机系统的目的。但一般来说，网络犯罪分子的主要威胁对象为网络安全意识较淡薄的个人用户，给这部分个人用户带来了经济损失。

3 计算机网络信息安全的防护措施

3.1 防火墙技术

计算机网络中的防火墙技术，主要监视内部网络与外部互联网之间的联系状况，能利用企业所设定的安全防护策略对内部局域网进行保护，以防止外部网络中的病毒入侵内部网络，而现代防火墙技术则主要包括了软和硬件两部分，对进出内部网络中的数据进行严格监控，以防止非法入侵、恶意代码的入侵，由此达到保障内部网络数据的安全性，而现代防火墙技术通常都具有了安全告警、部署和转换内部网络地址等功能，并且还能对正在上网的内部用户情况进行监视，对安全实施保护的功能，以此实现提高内部安全系统的性能，并能够限制内部用户对外部网络、站点访问的功能，对于改善内部安全系统有着非常关键的意义，由于防火墙的功能众多，需要针对具体的情况进行选择，一般情况下，需要采用一种的防火墙方式，对整个互联网进行防护，常见的防火墙方式。利用防火墙可以对内网络进行集中安全控制，并根据网络的具体要求，设置适当的安全防火墙措施，使内防火墙的整个防护体系中的每一位计算机都能够分别正常地运行，同时还能够根据网络内部的特点，对网络中的流量进行检测，便于对网络中的流动数据进行监视和管理，或者改动将某个程序集中存放在防火墙内，以便集中对整个网络系统中的数据实施安全防护[1]。

3.2 加强网络信息的加密处理

随着互联网应用速度和规模的不断扩大，为了尽可能的降低黑客攻击事故的发生率，就必须要实施更加科学的数据加密管理，并以此来加强对计算机中的一些重要信息和私密数据的保护与管理，从而使其破解与攻击技术难度的范围逐步扩大，这样就最大限度的降低了对攻击者产生破坏的成纪概率。所以，人们在使用计算机网络过程中，应当根据计算机网络的具体运行状况，以及根据影响计算机系统安全技术的有关原因，采取一些较有针对性的公用加密，或者私用加密方法，由此可以有效防止中国计算机系统的关键信息遭到了一些非法操作人员的侵犯与窃取，也有利于中国计算机网络领域重要机密安全技术保障能力的提高，并使所获得的重要资料与信息具备了较高的安全系数和可信度[2]。

3.3 建立科学合理的备份与恢复功能

连接给定的属性，以及网络服务器便是属性安全控制，通过对比权限设定，能够提供网络安全上最深入的保护。网络属性不仅可以更高效的删除、拷贝和记录，还可以更高效保护在某些关键目标中的文档，并可以由此来保证其重要的执行目录和文档，没有被非法人员故意修改或者删除。同样，通过利用备份系统，也可以对某些关键存储设备的非正常损毁，进行良好的避免。

3.4 培养和提高用户的安全意识

首先，提高了对计算机软件经营者的保护。同时计算机软件运营商也应该加大在电脑网络安全领域的投资，而不能产生侥幸心理，不给计算机的黑客系统带来可趁之机。同时由于电脑时常会遭到外部的入侵，而消

费者们又会对电脑的稳定性与安全产生着疑虑，所以如果适时做好了计算机的网络安全管理工作，不但能够降低了后期维修时所形成的投入成本。同时，也能够提高消费者对计算机软件公司的信任度，从而增加转机软件公司的品牌效应[3]。其次，提高消费者的保护意识。要让消费者意识到，不管自己是何人物都是作为黑客的攻击目标，都可以导致个人信息的泄露。而不法分子可能根据自己的个人信息去进行某些犯罪行为，所以一定要加强个人信息保护教育。

3.5 完善计算机网络系统

要比较好的处理计算机安全性方面，需要从一些方面入手，主要是安全性层面的问题，需要合理的做好计算机安全性方面的工作，从而提高我们所用计算机的安全性。同时也可通过构建良好的网络宣传渠道，进而提高用户的个人使用安全意识，从而促使更多用户了解到电脑安全的重要作用。

3.6 强化计算机网络系统的安全防御能力

提升中国计算机企业的网络安全保护水平，也是保障中国计算机信息安全的重要措施之一。首先应该增加人们对计算机软件安全管理的关注和重视，积极下载各公司所发布的正版软件，并定期更新应用软件，以使应用软件的使用性能和安全特性得到更全面的提升和完善。然后就是人们应该按照自身在计算机上的实际使用方式，对其中的重要数据信息做好备份，以避免因为计算机遭到攻击或是侵入，而导致重要数据信息损失，造成无谓的经济损失。而关于普通用户来说，则需要针对自己计算机系统的实际情况，选择云备份或者通过U盘方式进行备份。在当前的云备份产品中，现阶段也存在了很多较为先进的备份手段，如苹果的Icloud、百度网盘等，都是目前较为常见的备份方式，使得许多普通用户也可以针对自己的具体需求，对设备中的数据资料进行了更加高效的保护，进而避免了信息丢失问题[4]。

3.7 风险评估和风险管理

就整个计算机网络系统来说，对其实施安全评估的第一个意义就是要规避掉可能产生的安全危险，这也是提高互联网安全水平的必要条件。而针对风险管理工作而言，它的关键作用就在于利用与脆弱性分析、攻击意图分析等技术互相融合的方式，来防止了网络上重大安全隐患的产生，而网络扫描工具就是以能够利用这一技术方式为前提，对网络安全中的脆弱节点、以及安全隐患进行了查找，可以全方位地确保对每个存在的安全隐患都得到了合理的评估与管控。

结语

综上所述，由于数字化社会的不断发展，计算机科学早已深深地改变到了人们生活的方方面面。所以互联网技术人员必须对安全现象开展广泛的调研，并不断更新安全防护的管理措施，以提高自身防护意识，并通过教育的方式提高对网络的安全意识，防范网络诈骗和违法犯罪等情况，并从多角度采取了相应的管理措施，对网络中的安全问题进行了相应的防护，以维护计算机网络行为和数据的安全稳定性，给人们创造一种安全便捷的上网条件，从而推动民生质量的持续改善，推动经济社会的持续发展。

参考文献

[1]荀莎莎.计算机网络安全技术的影响因素与防范措施[J].科技资讯，2021，19(13):32-34.DOI:10.16661/j.cnki.1672-3791.2104-5042-8917.

[2]段聪影.计算机网络安全技术的影响因素与防范措施[J].信息记录材料，2021，22(05):60-61.DOI:10.16009/j.cnki.cn13-1295/tq.2021.05.032.

[3]於肇鹏.计算机网络安全技术的影响因素与防范策略分析[J].无线互联科技，2021，18(20):21-22.

[4]吴晖.计算机网络安全技术的影响因素探索[J].无线互联科技，2021，18(20):78-79.

[5]雍岐剑.关于计算机网络安全技术的影响因素与防范措施[J].网络安全技术与应用，2021(06):150-151.