计算机网络信息安全及防护策略研究

王向前
河南省中豫工程咨询集团有限公司　河南　郑州　450000

摘　要：当前，中国的计算机网络技术比较完善，计算机网络技术的使用范围不断扩大，民众对电脑安全的关注度不断增加。针对现如今存在的网络攻击、计算机病毒、互联网犯罪等网络安全威胁，本书还提供了安装的补丁程序，以便于做好入网安全管理工作；并提高了密码难度，以增加对访问网站的安全控制；有效部署了网站防火墙，以构建安全的防护体系；并通过政府监控，完善了互联网安全的防御对策，以期通过行之有效的防护策略，解决我国计算机网络信息安全面临的问题，营造健康和谐的计算机网络环境。

关键词：计算机网络；信息安全；防护；策略

引言

经济增长速度加快，带动科学技术的发展。作为制造和应用电脑的国家来说，中国从很久以前就开始启动电脑网络安全机制研发，而且已经获得较好成效，从总体上增强网络安全保障能力。人们在享受计算机网络信息带来便利的同时，也不得不面对由计算机网络产生的信息安全问题。作为制造和应用电脑的国家来说，中国从很久以前就开始启动电脑网络安全机制研发，而且已经获得较好成效，从总体上增强网络安全保障能力。但随着现代化社会的发展，威胁计算机安全的原因将日益增多。本章就电脑安全与防御技术进行简要阐述。

1 计算机网络安全概述

计算机与互联网在中国政治、经济和人文等领域都具有着巨大的影响，中国也是一个计算机制造与应用强国，据《中国互联网络发展状况统计报告》的发布数据，二零二二年，中国网民规模将达到10六十七亿，对计算机与网络信息安全存在着巨大的压力与挑战。计算机与网络信息安全涵盖了众多的应用领域，在经济应用领域，由于计算机网络和经营者的紧密结合，能够有效节省人力成本，为企业经营者提供了便捷的信息安全支持，以确保企业网络生产运营的有序管理[1]。在政治方面，必须加强互联网安全，才能确保国家机密不被盗用，也才能保障我国的政治建设和基础设施事业顺利开展；在文化方面，计算机与网络信息安全对社会文化资源的共享和艺术交流活动产生了直接危害。所以，提高计算机安全性，有助于提高社会文明的多样性近年来，国家也成立了计算机安全机制，全面启动管理计算机系统安全和保护的关键技术研发工作，在计算机硬件、网络安全软件、大数据保障等方面，也投入了巨大的人力物力与资源并做出了一定的应用，提升了计算机网络的安全系数，提高了网络安全保护水平。尽管如此，当前计算机系统安全保护系统还没有完备，危害计算机系统安全的各种因素依然存在，所以，要完善计算机系统安全管理系统与保护技术促进社会的发展进步，创造良好的社会氛围，展现社会精神面貌。

2 计算机网络信息安全的威胁分析

2.1 计算机以及网络技术存在问题

计算机网络安全出现问题的一个根本原因，是由于计算机本身的问题以及网络安全技术有待改善，主要表现在计算机硬件的容易损坏、计算机信息系统易混淆，以及个人信息也易于损毁等。电脑是信息载体，计算机本身的问题直接造成电脑安全无保障。互联网技术目前面临的主要问题是互联网技术发展速度较快，但互联网技术的主要特征就是开放并且保障了用户的信息流动自由，但在信息流动过程中由于缺乏实际的技术防护体系以及保护，如果发生了互联网瘫痪或是因为线路问题信息就会流失，这对企业来说存在着很大风险，对社会的发展来说也是亟待解决的问题。

2.2 黑客病毒攻击以及用户安全意识欠缺

黑客及其病毒入侵计算机网络是一个普遍的数据盗窃及破坏手段，黑客及其病毒可以进行入侵计算机网络的最大问题在于缺乏较为完善的、强大的防护技术，黑客可以较为简单的读取程序、控制数据流动、获取和篡改信息等。具体操作是，骇客通过垃圾邮件和各种邮件传播方式，将装有病毒的邮件传送到自己的计算机或者网络中，在用户接触和浏览过程中就能够很快的了解该应用的基本信息，甚至整个计算机系统的信息，在此之后造成的结果是非常不好的。网民意识不够这是一个严重的问题，很多人在互联网应用环境中对于必须注意的事项以及必须避免的行为都不知道，对需要填取的个人

真实资料甚至密码信息没有予以重视，或者缺乏一定的保密能力，这些都使得犯罪犯罪分子有隙可乘，以至发生难以挽回的情况。

2.3 电脑病毒的影响

近年来，计算机病毒的数量日益增加，风险日益加大，对计算机系统安全构成了十分致命的威胁。计算机病毒通常具有隐蔽性、潜伏性、存储性、可执行性、高感染性、低破坏性等特点，在通常情形下，计算机病毒都可以通过硬盘驱动器、软盘、光网盘、网络等多渠道传播[2]。而在具体的计算机程序运行过程中计算机病毒可以触及并渗入数据档案内部，从而导致整个计算机系统的混乱；同时，计算机病毒还可以通过拷贝和传递文件、运行计算机程序的途径传染，小的计算机病毒能够对计算机程序的工作效率形成影响，危害性较大的病毒则可以迅速损坏或者删除档案，导致关键信息的丧失，造成巨大的损失后果。

2.4 垃圾邮件和有组织的电脑犯罪

电子邮件具备了系统性、公开性、可广播性等的优势，为我们传递个人数据、文档信息创造了重要的途径与工具。但是，近年来，由于垃圾邮件数量越来越多，对中国人民的正常生活和工作环境产生了一定的负面影响和干扰。垃圾邮件发送者往往会先盗取目标用户信箱数据，进而把广告或垃圾邮件强制发送到用户信箱，以让目标客户接受。这些垃圾邮件中可以带有计算机病毒信息，一旦接收人在不知情的状态下贸然开启电子邮件，将给客户的电脑安全带来诸多风险。

2.5 网络使用人员操作技术不佳，容易产生安全隐患

除了前文提到的网络软件设备不全问题，产生网络信息安全的问题还容易受到网络使用人员的影响。如果计算机网络使用人员的操作技术不强，不能正确的使用网络开展具体的网络活动，这也可能会导致操作的失误。再者，如果网络使用人员不能对重要的网络程序和信息实施密码防护，则一些不法的计算机黑客很容易进入该网络系统，他们或许会篡改计算机网络中的重要数据，甚至是窃取关键的个人信息，而上述问题的出现，会造成很大的互联网安全风险。

2.6 网络硬件风险方面

在计算机网络使用过程中，硬件风险也是其中的一个很常见的方面，它一般指的是由于一些具有错误思想的人，对计算机设备的实施了入侵或者破坏，又或者是计算机在实际的应用活动中，遭遇了一些突发风险，这也使得计算机网络的硬件管理方面出现了困难，关键的网络数据很容易丢失，重要的网络信息容易流失，网络风险扩大[3]。再者，还有部分电脑并不能安装适当的防雷设备，一旦出现电脑断线、器件老化的情况，会导致计算机的损坏，也会给电脑安全造成一定的消极影响和阻碍。

3 计算机网络信息安全防护策略分析

当前，提高计算机系统安全保护已成为现代电子政务网络管理与安全网络平台建设的主要任务。做好网络安全工作，就是要始终以保证网络持续、安全、稳定运行为目标，着力维护计算机网络信息系统的软、硬件和U盘、光盘等储存设施计算机上的关键资料和信息，防止计算机网络及有关资料信息发生故意或偶然的损失、泄漏和损毁。文章提出，做好电脑安全防御，从如下角度出发，积极采取相应对策：

3.1 安装防火墙防治病毒入侵

计算机用户通过设置防火墙可以极大的提高安全保护的效率与质量，同时也能够有效外界不法分子对内部的网络进攻从而提高计算和网络的运行稳定性和保护性能。防火墙还可以对计算机上和互联网中的IP地址进行修改和调整，把常用网址转换为临时网址，这样就可以比较有效的阻挡病毒木马进入计算机了。而通过使用和设置计算系统和防火墙，就可以对在计算机硬件上、和互联网上出现的问题在第一时间加以识别和解决，使安全风险有效地消除，进而保证了计算机在安全可靠的网络环境中运行。

3.2 数据加密技术的使用

计算机安全性下降的主要原因是由于系统在重要的环境中容易受到骇客的非法入侵。所以，信息加密技术的应用可以在一定程度上保护使用者的数据安全，防止关键资料信息被不法分子盗用。另外还能够采用数据压缩方式，能够有效的减少信息占用的存放空间，对于比较重要的数据资料也能够提供备份功能，提高了客户重要信息的稳定性。计算机安全保护还能够通过数字签名方式对客户上传的数据资料进行实时的保密管理，这就可以提高客户资料的保密与安全，提高客户的电脑安全。

3.3 及时安装漏洞补丁程序

硬件、软件、系统中因功能不足、设置不合理而产生的问题和缺陷，常常给互联网骇客等不法分子的网络攻击和病毒入侵提供了机会[4]。“金不足赤”，在当前的计算机应用程序和操作系统中，都或多或少的会存在着某些漏洞或者缺陷，对计算机系统安全造成了极大的危险和隐患。针对这类问题，计算机软件制造厂家专门开发了电脑漏洞的补丁程序，能够更有效的预防由于缺陷而造成的计算机系统安全性危害。所以，在电脑使用过程中，请先使用金山毒霸、360安全卫士等应用软件扫描

并加载对漏洞的修补功能，再加以安装完善后，为计算机安全打造起新的安全屏障

3.4 保护账号安全

帐号权限被盗用也是数据流失的主要问题，因此建议采取用户注册保护，设置有效期限的办法来保护帐号权益。使用登录保护措施，通常采取的都是对已注册用户限制，如用户注册时最常见的方法是使用用户名、密码等的方式登录计算机，但在通常情况下，用户所注册的IP地址也不受限制这也为计算机黑客的侵入带来了方便，所以，必须用其他IP登录，并选择可以登录的工作站，并保存登录密码。其次确定好有效注册时间，因为默认系统的账号注册日期是永久的，这样一来，一旦账号被盗了，计算机信息体系就容易因此漏洞，不利于互联网安全，但是，也可以设定帐号的到期日为一周，甚至零点五个月等，而一个月后账户就需要再次注册，通过这个方法，就能够减少个人信息泄露风险，从而增强了计算机网络的安全。

3.5 建立计算机网络安全防护系统，加强计算机网络访问控制

完善的计算机网络安全防护系统是信息保护的关键，计算机相关部门要全面调查计算机网络信息安全及防护管理工作现状，找出计算机存在的漏洞，并对其进行分析，从而建立起严格的网络管理规范，做好病毒检测与网络监控，及时发现网络信息漏洞所在，做好安全控制工作，提高计算机网络信息安全防护工作的有效性。在此基础上，必须做好使用者自己的管理工作，用户必须管理自身的互联网使用行为，防止由于自己使用错误所导致的数据泄露。玩家们在使用电脑的同时，还应开启杀毒软件和防火墙，以确保安全，在操作过程中，要严格控制好自身的操作系统，以防止因操作过程中误点而所引起的数据泄露。此外，应定期清除访问数据，适时关掉网络接口，以此来增强使用稳定性。

3.6 根据网络实际情况，加强计算机网络信息管理控制

除硬件设施、应用软件这二个方面的管理与监控，相应的计算机网络管理监控也是很关键的方面[5]。通过设置科学的计算机网络系统，可以为计算机网络工作提供支持，也可以为网络信息安全提供保障。此外，各工作单位都必须加大对计算机系统及其应用工作人员的技术培养力度，提升工作人员的整体素质，以降低计算机风险发生的几率，不仅如此，信息管理各方面的工作人员，都应根据具体的方案加以实施，建立人员之间相互交流的纽带，对计算机网络系统实施定期的安全性检查，同时也要加大对各方面工作人员的技能训练和职业道德培训，以提高计算机及网络信息系统的安全性。

结语

互联网的变化更新速率很快，因此仅仅采取一种防御策略并无法满足网络时代下对互联网信息的安全。该文重点阐明了中国计算机信息安全保护的重要意义，同时建议使用补丁软件，进行入网安全检查工作[6].增加密码难度，提高登录网站速度；配置防火墙，建立网络安全防护系统；通过政府监管，建立互联网安全的保护措施。希望通过先进的信息技术来建立起计算机网络安全保护制度，促进中国计算机网络信息在安全的环境中发展。

参考文献

[1]朴新新.计算机网络信息安全及防护策略研究[J].中国高新技术企业评价，2016（7）.

[2]王红梅，宗慧娟，王爱民.计算机网络信息安全及防护策略研究[J].价值工程，2015（1）.

[3]史源.计算机网络信息安全及防护策略研究[J].计算机光盘软件与应用，2015（1）.

[4]刘艳丽.计算机网络信息安全及防护策略研究[J].中国科技纵横，2014（9）.

[5]孙志民.计算机网络信息安全及防护策略研究[J].电子游戏软件，2014（14）.endprint

[6]张璐明.大数据时代计算机网络信息安全及防护策略分析[J].网络安全技术与应用，2021（03）：153-155.