计算机网络信息安全及防护策略探究

孟建雷

北京中电飞华通信有限公司 北京 100160

摘 要：现如今互联网技术发展日新月异，计算机已经成为人们日常生活中必不可少的一个用品，同时在各行各业的应用范围也越来越广泛，已经成为人们工作和生活中最为重要的一部分，因而越来越受到大众的关注和重视。虽然此项技术发展迅猛，但随之而来的则是各种信息安全问题的出现，个人信息泄露事件屡见不鲜，因此加强计算机网络信息安全迫在眉睫，需要从根本上消除信息安全隐患，通过有效的措施，最大限度保障计算机网络信息安全，营造一个健康的网络环境。

关键词：计算机；网络信息安全；防护策略

Research on computer network information security and protection strategy

Jianlei Meng

Beijing CLP Feihua Communication Co., Ltd. Beijing 100160

Abstract: Nowadays, with the rapid development of Internet technology, computer has become an indispensable article in people’ s daily life. At the same time, it has been more and more widely used in all walks of life and has become the most important part of people’ s work and life. Therefore, it has been paid more and more attention by the public. Although this technology is developing rapidly, it is followed by the emergence of various information security problems, and personal information leakage incidents are common. Therefore, it is urgent to strengthen the computer network information security. It is necessary to fundamentally eliminate the hidden dangers of information security, ensure the computer network information security to the greatest extent through effective measures, and create a healthy network environment.

Keyword: Computer; Network information security; Protection strategy

现如今已经处于信息时代，因而计算机网络技术的使用率也越来越高，毫不避讳地说，此项技术已经与人们的生活和工作完全离不开了。正是因为有了此项技术，才让人们的生活变得更加的便捷，让人们在处理工作时更加的方便，促进了工作效率的提升。但需要注意的是，任何事物都有双面性，计算机网络技术虽然让人们的生活与工作变得更加简便，但是由于其自身的开放性，使得其在使用过程中容易发生信息安全隐患，危害信息安全，因此，加强此项技术的防护就成为当前最重要的事情。

1. 计算机网络安全的概述

随着现代通信技术和计算机技术的发展，计算机网络应运而生，就其本质来讲，计算机网络在现实中不存在实体，而是一个虚拟空间体系，它可以将各个地方的计算机设备连接起来。随着技术的不断进步，信息技术的发展也日新月异，与人们工作和生活也变得日益紧密，对于行业的发展带来了积极地影响，社会的生产、生活越来越依赖此项技术。利用计算机网络信息技术，不仅可以资源共享，还可以对企业中所需的各项数据进行收集、整理和总结，提高企业的工作效率和生产效率，也可以在一定程度上扩大企业的经济效益，同时此项技术的应用也可以为企业的信息安全起到保护作用，促进其可持续发展，但是也应认识到计算机网络技术是把双刃剑，好的一面主要表现，第一由于此项技术可以资源共享，因而人们在获取数据信息时更为方便，而且大大缩短了收集数据的时间[1]。第二，可以促进人们的信息交流。坏处则主要体现在第一，缺乏有效的监督和管理，使得计算机网络存在安全隐患，而且最重要的一点的则是数据的泄露会给企业带来严重的经济损失。因此，要加强信息安全保护，针对安全隐患制定防护措施，保证计算机网络的安全。

网络安全从小的方面的来讲，可以维护社会的稳定，从大的方面来讲，对于国家的数据安全也具有重要的作用。此项技术的涉及的内容较多，包含通讯、密码技术等多个领域。保证计算机网络的安全，就是保证信息的安全，保障财产的安全。但是在现阶段，公共计算机网络存在着较多的安全隐患，威胁信息的安全。因此需要应用网络安全技术对计算机网络进行防护，确保信息不会遭受泄露的风险，同时也能避免有害信息的传播。

2. 计算机网络信息安全问题分析

2.1 计算机病毒

什么是计算机病毒？指的是不法分子利用此项技术，人为地制造出一些应用程序，利用文件或者是数据进行复制传播，对信息安全造成威胁，而且这种有害的应用程序较为隐蔽，一般很难发现。据调查和研究数据指出，计算机病毒危害性极大，不仅会造成数据的泄露，同时还会对计算机本身的硬件设施造成严重的影响，若情况严重，可导致整个系统瘫痪。计算机病毒主要具有以下。第一，潜伏性。计算机病毒在进入系统之后并不会马上就开始运行，可以在系统里面潜伏很久，短则几周，常则可达几年，通过隐蔽在合法文件里，威胁其他文件的安全，对其他合法的文件进行传染，只有达到要求时，才开始露出真面目，对数据及整个系统开始进行破坏，

而且病毒在计算机里面的潜伏的时间越长，则危害性越大，破坏性也更强。第二，传染性。这个特点是病毒最为基础的特点，通常判断一个计算机系统是否具有病毒就是以此为依据的。而且由于病毒的此项特点，使得其可以通过多种方式 向其他正常运行的计算机进行扩散，导致其他正常的计算机系统因病毒而瘫痪。现如今计算机网络发展迅猛，病毒传播速度与以往相比也更加的迅速。第三，破坏性 [2]。计算机病毒也具有强大的破坏性，可以自行对文件和系统的数据进行篡改，而且可以中断系统的正常运行，而这也是病毒设计者的最终目的。第四，可触发性。病毒的设计者在对病毒进行设计时，设置了触发标准，只有达到条件时，病毒才会开始运行。若触发条件一直未被激活，病毒就将一直潜伏在计算机系统之中。

2.2 黑客攻击问题

随着计算机技术的普及，如今能熟练应用计算机技术的人数与日俱增，但在当前的环境中，部分人为了一己之私利用自身的技术优势，对其他数据进行破坏和修改，以此来获得利益，而这部分人也有一个专有的称呼，黑客。对于黑客攻击来说，使用率最高的则是口令攻击。由于计算机管理员自身安全意识不强，在设置口令时经常使用同一个密码，或是设置的口令太过简单，使得黑客可以轻而易举地利用口令破解软件进行破解。其次则是恶意代码和后门程序攻击。恶意代码就是在日常生活中经常听听的病毒、木马等，后门程序则是指黑客对系统进行攻击后为了方便其在此进入系统而预留的隐蔽通道 [3]。还有则是操作系统漏洞。黑客可以通过专门的黑客软件对系统的漏洞进行攻击，或者利用各种欺骗手段对用户的使用权非法获取，进而达到控制系统对系统进行破坏的目的。除此之外，还有拒接服务类攻击和缓冲区溢出，也是黑客攻击常用的手段。

2.3 计算机网络安全管理问题

信息问题的安全越来越受大众的关注和重视，而在大数据时代的背景下，绝大多数信息数据都是通过网络进行传输的，因此网络安全已经成为研究的重点和热点。计算机网络安全管理出现问题，主要在于程序人员在对软件进行编码时，存在一定的漏洞，使得黑客可以利用软件的漏洞进行破坏。人为因素也是原因之一，管理员的安全意识缺乏，且受年龄、文化水平等因素的影响，在进行安全设置时，口令设计过于简单，以生日或是身份证号为密码，导致很容易被破解。或者是未安装专门的杀毒软件，也在一定程度上增加了安全隐患的发生风险。此外则是网络硬件的配置存在问题。在对网络进行配置时，考虑不全面，配置较为落后，使得其协调性较差 [4]。而且在计算机投入使用之后，管理人员并没有定时对其进行检查和维护，导致出现的安全漏洞无人处理，最终引发安全问题。还有则是管理制度不健全。未对管理人员的日常工作进行监督和管理，使得其对待工作缺乏积极性，还有在防火墙的设置上，未仔细检查，使得访问权限被扩大，导致其被滥用而造成安全问题的发生。

3. 计算机网络信息安全问题的防护策略

3.1 计算机用户层面的防护策略

3.1.1 提高计算机网络信息使用者的安全意识。

计算机的网络安全与使用的安全意识具有很大的关系，并且安全问题也与使用者本身具有一定的联系。在开始对计算机进行操作时，使用者必须认真阅读计算机的使用方法及操作步骤，需要着重注意计算机操作的注意事项。按照规范的流程对计算机进行操作，若在操作过程中有任何的问题以及时请教。避免因自身的问题而增加计算机的使用风险。同时需要使用人员全面掌握计算机可能存在的问题及风险，告知其不会操作的地方可以就像他人询问，在操作过程中对于为未知的链接切勿进行点击，对于不认识的软件也切勿进行下载，可以在一定程度上防止病毒的入侵。除此之外，加强计算机使用者对计算及相关知识的学习，增强使用者对计算机的了解，规范使用者的操作流程，提升计算机安全意识，拓宽关于计算机的知识面，培养健康的计算机使用习惯，最大限度保证计算机网络的使用安全 [5]。

注重软件的选择，积极选用安全绿色的软件。为了保证计算机的安全，在对使用的软件进行下载时，应对软件进行甄别，并且要在合法的平台对软件进行下载，切勿点击网页的不明链接对软件进行下载，此举可以降低病毒的感染率。此外，用户还必须加强自身的识别能力，对软件是否正规、是否合法、质量的优劣进行鉴别，若自身的鉴别能力较差，可以以软件的评价作为参考，确保下载的软件不仅正规，而且质量好。对于计算机，要想保证其安全，则最为重要的则是对杀毒软件的选择，以及防火墙的安装。杀毒软件的作用的在于可以发现病毒，对病毒进行检测，待检测到病毒后，可及时将其消除掉，保证计算机的安全。防火墙的存在可以对不明访问进行拦截，可以对病毒起到预防作用。待杀毒软件安装成功以后，应定期对计算机进行杀毒，确保计算的安全，避免其受到有害程序的入侵。同时技术人员好需要根据病毒的发展以及用户的需要有针对性地对软件进行开发，提高软件的杀毒效果。

此外，加强对账号的安全保护。计算机网络包含着用户的个人信息，一旦被盗取就容易造成巨大的损失。现阶段各种应用程序层出不穷，不用的程序有不同的个人账户，程序越多，人们的个人账户越多，部分用户为了方便，将所有程序的个人账户都设置成一样的，因而很容易被破解，进而对个人或者是企业造成经济损失。针对这些个人账户，用户应该加强自身的安全意识，提高对账户的安全保护，例如在设置密码时，切勿将密码设置成最直接的生日等较为简单的数字，或是单纯使用字母密码，在进行密码设置时，尽量将其设置得更为复杂一些，可以将字母、数字、字符联合使用，这样可以提高密码的复杂程度。此外，对于账户的安全管理，在陌生的环境登录个人账户时，在使用完毕后应立即清除个人的登录信息，此举可以自大限度加强对个人的信息安全保护。

3.2 计算机网络信息技术层面的防护策略

3.2.1 入侵检测技术

此项技术通俗的话来讲，就是对计算机的本身环境进行 24 小时的检测，防止病毒的入侵，并且对于病毒的入侵可以自动采取预防措施，确保信息的安全。入侵检测是针对计算机内部进行检测，而之前提及的防火墙则

是对计算机的外部环境进行检测，对外网存在的安全隐患进行排查和预防。入侵技术对于计算机网络安全的作用非同小可，不可忽视，必须引起重视。

3.2.2 信息加密技术

在通常情况下，为了保证信息的安全，可以对计算机的数据及信息进行加密处理。何为加密呢？就是将需要加密的信息转换成密码文字，以提高数据信息的安全性，通俗地讲，就如同将一大笔现金放入保险箱。通过加密，使得不法分子对加密后的信息无法正确识别，就算窃取了相关信息，也无法进行破解，确保了信息的安全，同时也使不法分子窃取信息的难度不断增加，提高了计算机的可靠性。现目前，使用率最高的有两种加密方式，一种为公钥加密，另外一种则为私钥加密，加密方式不同，则其使用方法也有所不同，但都具有共同之处，可以保证数据信息的安全，防止信息被盗取。

3.2.3IP 地址隐藏处理

为了提高信息的安全性，用户使用计算机时，可以对自己的 IP 地址进行隐藏。现如今技术发展日新月异，用户在传输文件时也可以将自身的 IP 地址进行隐藏，将 IP 地址隐藏后，即使不法分子将信息成功盗取，也无法对信息进行破解，从而也使得其无法利用盗取的信息。而且，最重要的是，用户在发现自己的信息被盗取以后，可以最短的时间内修改自己的信息，保证计算机的安全。

3.2.4 防火墙技术

要保障计算机网络信息安全，还需加强防火墙技术。以往的防火墙技术存在较多的缺陷，对于数据的检测并不全面，仅对进入系统的数据进行甄别和过滤，因而还是存在较大的安全隐患。如今计算机技术发展势头正猛，计算机病毒及黑客攻击的技术也在不断地升级，因而需要对防火墙技术进行完善，实现全方位的安全技术集成。同时也要加强对防火墙的有效利用。例如在企业中，计算机应用十分普遍，可以说，没有计算机的存在，可以让企业寸步难行，这是因为计算机应用涉及大量的数据信息，因而也容易受到黑客的青睐，因此，为了保证企业信息的安全，减少安全风险及经济损失，需要提高对防火墙的利用率，建立健全信息安全防护制度，从源头上提高管理人员的安全意识及防范意识。而且如今正处于大数据时代，为了有效抵御黑客的攻击，需要加强对防火墙技术的利用，利用其自身优势对不良软件进行干扰，提高网络运行的安全性。除此之外，要定期对防火墙技术上进行维护和检修，确保其处于正常运行的状态。如今技术发展多种多样，病毒的类型也多种多这样，因而需要技术人员加强学习，了解更多的病毒知识及其特点，性能够针对不同的病毒制定相应的防范措施，全面保证计算机网络信息安全。

3.3 网络安全管理层面的防护策略

3.4.1 完善相关的监管机制。

建立健全监督管理的制度可以营造良好的网络运行环境。规范的制度是保证信息安全的基础，因而国家应根据网络发展的实际情况制定并出台相关的法律法规，对违反信息安全的行为作出严格的界定并进行严肃的惩处。从企业层面来讲，也应该对计算机的使用流程制定相应的操作标准，规范人员的使用流程，减少安全隐患，同时作出严格的规定，在计算机的使用过程中若发现信息安全隐患，应立即报告给技术部门，便于技术部门在最短的时间内进行处理，此举可以防止信息被泄露和盗取。此外，还需制定网络信息安全预警机制，提高计算机网络信息安全的预防能力。

结语

总而言之，我国计算机技术已经走在发展的前端，与以往相比，已经变得十分发达，但发达的背后带来的则是信息泄露事件屡禁不止，不法分子为了个人的利益对用户的信息进行盗取，使得用户或者是企业蒙受巨大的损失。计算机技术的发展虽然为人们的生活和工作带来了便利，但随之而来的则是各种信息安全隐患的发生。因此为了保证计算机网络信息安全保护，需要采取行之有效的措施对其进行预防和控制，例如对提升用户的安全意识，加强对防火墙的使用、安装杀毒软件等，都可以在一定程度上提高信息保护的安全性。同时也可以建立健全相关的制度，通过制度规范营造一个健康的网络环境。

参考文献

[1] 李长挺 . 信息化背景下计算机网络信息安全防护策略 [J]. 电子世界 ,2022(01):146-147.

[2] 章菊广 . 局域网环境背景下的计算机网络安全技术应用策略 [J]. 网络安全技术与应用 ,2022(01):2-3.

[3] 姚玉开 , 赵杰 , 陈洋 . 浅析计算机网络安全技术的影响因素与防范措施 [J]. 中国设备工程 ,2022(01):235-236.

[4] 杨佳兰 . 基于大数据环境下的计算机网络信息安全与防护策略研究 [J]. 南方农机 ,2021,52(23):132-134.

[5] 邹佳彬 . 顾及大数据聚类算法的计算机网络信息安全防护策略 [J]. 电子技术与软件工程 ,2021(18):237-238.

作者简介：（198202）男 汉 山东菏泽市 项目经理 现主要从事的工作或研究的方向：主要从事计算机网络安全和系统运维工作