计算机网络信息安全管理及防护

赖国雪
承德钢铁集团有限公司　河北　承德　067002

摘　要：随着计算机网络的不断发展普及，其与人们的生产生活越来越密不可分，但是由此带来的信息安全隐患也随之增加，对计算机网络的持续发展以及人们的生产生活造成不良影响。本文以计算机网络为切入点，分析目前信息安全存在的隐患，并浅析如何针对这些隐患进行防御，以通过对信息安全问题的研究来为计算机网络用户营造一个更为安全的网络使用环境。

关键词：计算机网络；信息安全隐患；安全防御

引言：随着经济的发展和技术的进步，人们的生活越来越离不开计算机技术。计算机在改变行业发展规律的时候也改变了人们的生活习惯，由此社会进入了大数据时代。在大数据时代，人们很容易就能查到来自世界各地的信息，只要想知道就会有途径。这种对于信息搜集发现的能力导致了人们对于信息的获取变得容易。在大家进行信息搜集和相互交流的时候，每个人都会在大数据中形成自己的痕迹，这就有可能发生隐私泄露。在人们还没有反应过来的时候，不法分子已经盯住了大数据时代这一特点，将信息技术应用到盗取他人信息的方面，将人们的信息非法提取并从事对用户不利的行为。面对信息技术带来的便捷与风险，每个人都要树立一定的风险防范意识，从而保护自身的隐私和财产安全。

1 计算机网络概述

近年来，计算机网络技术得到了快速普及和发展，成为人们工作和生活中不可或缺的工具。企业的发展和运行更是离不开计算机网络技术的支持。财务管理、资产管理、生产管理、人力资源工作等都离不开计算机网络技术的支持。作为一门综合性很强的学科，计算机网络技术涵盖了通信技术、网络技术、密码技术等多种技术，是兼具理论性和实践性的学科。计算机网络安全运行首先要对软硬件采取严密的措施，在保护硬件安全的基础上保障计算机网络系统不受非法攻击和侵害，降低信息被损毁和泄露的风险。计算机网络带有自由、虚拟、开放的特点。计算机网络还具有高度共享性，使用者借助计算机网络，就可以获取相应的信息和资源。同时，计算机网络也衍生了隐患和风险，开放、虚拟和自由的计算机资源也给计算机病毒的入侵提供了可乘之机，一些不法分子通过入侵网络系统来盗取信息和机密，进而为网络安全发展带来隐患。一些非法网站为了获取相应的信息和资源，故意散播病毒，这给计算机网络安全带来很大的威胁。

2 计算机网络信息安全存在的风险分析

2.1 系统安全漏洞

在我们现有的操作系统及应用软件中，不可避免的会出现一些漏洞，黑客往往会借助于这些漏洞来开展攻击。系统安全漏洞是指计算机网络自身存在可威胁网络安全的软件、硬件设计缺陷或错误。因此，软件公司在开发产品的时候，不仅要开发软件，也要关注硬件，同时也要重视后期的软件测试工作，以便将存在的漏洞及时找出并科学完善[1]。

2.2 计算机病毒升级，危害越来越大

随着信息技术的发展和提升，越来越多的计算机病毒被制造出来，成为计算机网络安全的隐患。通常，在计算机的使用过程中，虽然适用性非常广泛，但其实存在一些兼容性和缺陷问题，这些问题增加了网络安全风险。同时，虽然计算机网络已经普及到了各家各户，但是操作人员的水平层次不齐，不规范的操作行为也会让计算机在使用过程中产生缺陷，从而破坏计算机的正常运行，这也为一些计算机病毒和不法分子的入侵提供了机会。此外，计算机系统是一种非常严格的编程系统，一旦遭受到来自外界的病毒入侵就会失去操作功能，降低使用的安全性，而病毒也随着计算机系统的升级越来越难清理和察觉。所以，经常会出现一些具有极大破坏性的病毒出现在计算机网络中。这些病毒会让用户的计算机在无形中受到感染、防不胜防。这些病毒最厉害也是最可怕的地方在于，一旦出现病毒感染，就有可能失去计算机中保存的重要信息，甚至破坏原有的计算机系统。这些病毒严重降低了计算机网络安全系数，成为计算机网络安全中重大安全隐患[2]。

2.3 内部管理引发的信息安全隐患

网络信息安全隐患不仅受到外部环境和内部系统的

影响，还受到管理制度的影响。首先是计算机相关的从业人员的操作不规范问题，如不对淘汰的废旧设备进行系统的技术处理，使得一些数据被披露。其次是网络管理人员没有遵守职业道德，利用自己的网络权限，对数据进行窃取或损坏，又或者非法提供访问权限，使得系统内部数据被泄漏。第三则是计算机网络的安全管理制度不够健全，没有严格的审批程序，监管也不到位。第四则是计算机运行环境，若计算机在一个不稳定的电压环境中，很容易造成数据丢失的现象，不利于信息安全的保护。

3 计算机网络信息安全管理与防护对策

3.1 提升网络信息安全意识

治理网络信息安全隐患，确保网络信息安全的关键性因素是“人”。首先，要积极普及网络信息安全知识，从思想层面加深对网络信息的深入认识。其次，要健全网络信息安全管理制度，明确管理人员工作职责，加强对管理人员明知故犯或操作不当的责任追究。最后，个人用户也要严格规范自身网络行为，自觉树立网络信息安全意识，自觉担负起维护网络信息安全责任，提高个人信息安全意识，通过安装杀毒软件、定期检查敏感文件、修补已知漏洞等手段确保个人系统安全。只有树立网络隐患防范的意识，才能从根源上治理网络信息安全问题[3]。

3.2 构建网络安全防火墙

在大数据时代，人们接收信息的来源多种多样，信息泄露的风险也越来越高。面对这样的信息使用环境，建立良好的网络安全防火墙能够在一定程度上增加信息的安全性。在如今的网络世界中，有一群精通信息技术但是心思不正的非法分子，在进行信息挖掘的时候就会专门盗取别人的身份信息，从而对个人进行威胁和锁定。面对这样的邪恶势力，建立防火墙就是一种非常有效的方式。网络防火墙是一种能够为网络提供屏障的安全保护系统。网络防火墙对于每个系统是不一样的，在不同的系统中可以有不同的防火墙，这就提升了防火墙的防范能力。在防火墙运行的时候，一旦发现有外来的非法数据进入就会启动防火墙功能，管理其他人员的访问权限，避免计算机内的资料被盗取。对于非法入侵的用户，防火墙会及时通知本机的用户，限制非法分子的使用，并拦截弹出的窗口，为用户提供安全的上网环境。因此，构建网络安全防火墙能够提高计算机的安全等级，为计算机的使用提供保障措施[4]。

3.3 增强日常检测

为了预防信息的泄露、保障用户的信息安全，用户可以在使用计算机的时候进行日常的检测，及时了解计算机的状态，为计算机构建良好的运行环境。对于现有的防火墙系统来说，只有在有非法用户入侵的时候才会启动抵御机制。而在计算机的日常使用中，保持良好的检测习惯，能够减少计算机感染病毒的风险和弥补现有计算机的薄弱环节。同时，在日常监测中，计算机往往能够识别过去出现过的风险，并且进行标记。就像骚扰电话标记一样，只要同样的风险出现，就要进行拦截。如果新出现的风险没有到达这个级别或者危险系数不强就可以不予以处理，这样一来，用户在使用计算机的时候就会顺畅很多，大大提高了用户的体验。这也就相当于为计算机构建了一个病毒风险库，让计算机在运行的过程中与这个库中的风险进行对比，只有符合了某些风险库中的标准才可以判断是非法入侵。所以，使用计算机的时候及时进行日常的检测是非常有必要的，能够保证计算机的顺利运行、提升计算机风险处理能力。

3.4 加大监管力度和宣传力度

当下，有关组织和机构对网络信息的保护力度或者说重视程度还不够。网络已经发展成一个庞然大物，信息被泄露可能会造成极为严重的后果，相应监管部门应给予足够的重视，投入足够的人力、物力来保障信息安全。网络世界的虚拟性可能会放大部分人内心的阴暗面，更容易做出犯罪行为，加大监管力度十分必要。同时，相关部门还应向广大网络用户多宣传网络安全的重要性，用户要时刻注意自己的信息安全。

结束语: 随着计算机的使用率的提高，安全问题也是刻不容缓。因此不管是个人还是集体了解计算机网络的防护就变得极为重要。相关从业人员应不断创新计算机网络信息保护技术，保障用户信息安全；有关部门应尽到监管的责任；用户应加强自身的安全意识，共筑一个安全的网络世界。

参考文献：

[1]衷奇.计算机网络信息安全及应对策略研究[J].江西：南昌大学,2010. 08(36):108-109.

[2]龙震岳,魏理豪,梁哲恒,艾解清.计算机网络信息安全防护策略及评估算法探究[J].现代电子技术,2021,38(23):89-93.

[3]王伟然,李芝语.计算机网络信息安全问题探讨[J].软件,2021,42(07):108-110.

[4]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.