# 计算机信息网络安全技术和安全防范措施探讨

黄 波
通号城市轨道交通技术有限公司 北京市 100160

**摘 要：**随着社会经济的高速发展与科技技术不断提高，计算机技术被广泛应用。在社会各行各业的发展中，计算机技术都发挥了重要的作用，人们的日常工作和学习都已离不开计算机技术。虽然计算机技术为人们带来了极大的便捷，但也造成了较大的安全威胁，因此，提高计算机的网络安全技术和防范措施，保证计算机的安全网路环境至关重要。

**关键词：**计算机；信息网络；安全技术；安全防范措施

## 1 计算机网络安全概述

一般来说，利用计算机网络系统的安全保护来避免计算机系统内的数据、硬件等遭到破坏，并且通过一些合理的管理以及技术方面的安全保护，来确保数据的完整性，使其避免恶意病毒的破坏，这就是计算机网络安全当中所包含的主要内容。在国际标准组织中，对计算机网络的安全定义如下所示：为数据处理系统建立起相应的安全保护，并且对计算机网络系统中的数据、软硬件等保护，使其避免恶意病毒的破坏。通常，网络安全以及信息安全都是计算机网络安全当中所涉及到的内容，在网络安全当中，最为主要的一点就是网络的运作以及网络之间的联系，而在信息安全当中，数据的保密性、完整性等方面就是其中最为主要的内容[1]。

## 2 计算机信息网络安全技术

### 2.1 数据加密技术

数据加密技术是常用的计算机网络防护技术，通过对信息加密，只有使用正确的密匙才能解开加密信息过去正确的内容，现阶段，数据加密信息有效的提升了用户信息的安全增加数据保护措施，有效的防止了计算机系统中的数据丢失。数据加密技术一般分为两类：一类是芯片组文本存储，另一类是访问控制技术，它的主要任务是对传输过程中的数据流加密，对有线数据一般采用哪种加密方式；以及一类是完整性认证技术，它的主要任务是对传输、访问和验证相关信息所涉及的数据符合保密要求。数字加密主要表现为密钥的应用。密匙管理技术主要包括密钥的生成、分配、保存和交换等安全措施。对数据加密功能了分析，有效防止机密信息的传输；同时，加密技术也广泛应用于信息认证、数据签名等领域，可有效防范电子欺诈的发生[2]。

### 2.2 防火墙技术

此项技术能在公共网络以及私有网络中有所使用，可以有效避免病毒对计算机造成的破坏，属于一个防御性的设备。此项技术可以对网络系统中的相关数据信息有效开展监测，判断数据是否安全，一旦不安全，防火墙就会对数据的相关运输线路拦截，避免其入侵网络系统。针对防火墙来说，其拥有一定的免疫能力以及抗击病毒入侵的良好性能。在的网络安全中已经开始广泛使用防火墙技术，其重点是经过对网络流量有效控制，从而更好地确保网络的有效性以及安全性。在防火墙技术中，网络一共涵盖两种，即非信任网络以及信任网络，随后对非信任网络有效实施访问管理。通常防火墙设置在网络以及外界网络之间的接口处，采取边界化的模式，对ARP数据包很好的筛选以及过滤，有效阻碍外界网络里面不合法的ARP数据包攻击学校的网络系统，使网络的安全性获得充分提升[3]。

### 2.3 防入侵技术

在对计算机网络安全问题防范的过程中,要加强入侵防护技术的有效应用,这是提高计算机网络应用安全的重要技术类型,也是当前计算机网络安全防护技术研究的热点话题。入侵防护技术在应用过程中可以搜集计算机网络系统的关键信息,对相关的信息分析和处理,在分析中能及时发现计算机网络系统内是否存在违反安全操作的行为或者计算机是否被攻击过。这样能对计算机的内部与外部入侵实时防护。入侵防护技术在应用过程中需要加强入侵检测技术的应用,这是提高其防护水平的重要基础。在实践过程中为保证入侵检测技术的科学性以及有效性,需要对网络信息技术、统计技术等结合应用,这样有利于及时发现计算机网络内的安全问题,提高入侵防护效果[4]。

### 2.4 病毒防护技术

因网络互联，致使病毒传播速度加快。所以，应及时阻挡病毒传播。在代理、SMTP、群件等服务器上安装过滤病毒的软件或在桌面安装监控软件。先采用防病毒

软件检查与清除病毒；更新病毒数据库，将其下载到桌面系统。在防火墙或PC上安装Java软件，不允许随意下载控件。而且还应做好数据加密以及身份认证等工作。采取人脸识别、指纹验证等方法认证用户身份，保证用户安全使用计算机。

2.5 安全隔离技术

安全隔离技术是指在计算机网络系统边界上设置安全隔离屏障阻却网络病毒、有害网址等的入侵。该技术是在计算机网络攻击方法渐渐加强的情况下，为满足对特殊网络应用的保护而出现的，在保障内网与特定外网之间信息数据交换安全方面具有重要作用。

2.6 身份验证技术

身份认证技术通过查证核实网络用户的身份，可以有效的防止非法用户访问计算机网络信息系统，现今行业内有HTTP身份认证和IP身份认证等常用身份认证技术，网络用户的身份在通过这些技术的认证后，经由服务提供者对验证信息予以审核通过后，用户才能在网上阅读浏览信息[5]。

2.7 漏洞扫描技术

信息系统漏洞的出现，多是由于软件更新、系统更新后，新版本软件与老系统的冲突，或新系统与老版本软件的冲突，导致漏洞。需注意，即使最新的软件与系统，也会存在相互间兼容性不佳、漏洞等问题，因此唯有不断软硬件的适配，才能保障功能更新迭代下，信息网络安全水平始终趋近于完美。而关于漏洞问题的解决，需要依赖于漏洞扫描技术。

该项技术能准确识别大多数的系统安全漏洞，为信息网络安全管理人员提供技术指引，在接下来更有针对性地围绕这一漏洞，予以系统性地解决。而漏洞扫描技术发展至今，基本一些搭载平台已经具备漏洞扫描与实时修复的功能，计算机信息网络安全防范领域走向自动化。现有的漏洞扫描类型为网络安全扫描与本地安全扫描两种，扫描工作需要双管齐下。

2.8 云安全技术

云安全技术是信息技术不断创新发展的产物，云安全技术近些年来在实际生活中的应用越来越普遍。云安全技术能保障计算机信息网络的安全性，把计算机用户的电脑和负责安全保护生产商的技术平台能绑定在一起，这样用户和安全宝生产商能形成系统网络，专业的生产商统一负责开展计算机信息网络的防护工作[1]。

## 3 计算机信息网络安全技术和安全防范措施探讨

3.1 加强网络安全建设

当下，资产安全建设仍是网络安全建设的中心，但近来资产漏洞问题时有发生，也引起了人们的关注，这是因为人们依然将资产安全的重点放在了威胁检测、安全防御等外围建设上，反而把资产自身安全的加固遗忘了。

资产的安全建设应是网络安全建设依据企业自身的资产，对企业的未知资产还有已知资产梳理和筛查，并结合所公开的业务、服务、应用、数据等情况分析，从而对资产的变化情况加深了解，能从漏洞检测、合规检测以及外部威胁情报分析等多个维度持续监控和分析。才能筛选出潜在风险，再根据其在风险设定相应的时间处理机制，保证在网络安全事故发生的情况下能有效地处理好相关事宜，将网络信息安全事故的消极影响降到最低。

3.2 提高计算机网络安全风险防范意识

网络安全风险防范意识提升主要针对用户计算机网络使用行为提出，用户在使用网络工具时，应做到不随意泄漏私人信息、不下载来源不明的软件、不盲目开启软件使用权限。开放程度高是网络环境的基本特征，想要对个人隐私有效保护比较困难，但仍要求用户具备足够的安全风险防范意识，尽可能降低安全风险发生的可能，合理维护自身利益[2]。当企业遭受网络安全风险时，带来的损失及影响往往更为严峻，建议企业将网络安全漏洞管理及风险预防纳入到企业日常管理体系当中，对内部系统访问权限严格限制，如移动存储设备应执行注册管理方案，使用加密认证取代用户名及密码登录，提高网络安全管理能力。另外，企业还可与专业的网络安全管理机构相合作，结合企业经营管理特点及计算机网络使用情况，帮助制定针对性的网络安全管理体系，确保企业内部信息安全。

在操作行为的管理上，企业用户应定期对人员开展计算机网络安全培训，形成良好的计算机操作习惯，禁止人员通过社交平台、门户网等散播秘密信息，禁止利用企业计算机访问不明网站或下载网络文件。定期计算机网络安全系统维护，更新杀毒软件，确保安全防护系统始终处于正常运行状态。相关人员在利用计算机工作时，还应养成数据备份及加密习惯，若发生无法避免的计算机网络安全问题，也能将损失及影响降到最低。网络信息的发布须由专人负责，对信息发布过程严格监管[3]。

3.3 加强计算机防病毒能力

计算机经常受到病毒的攻击，导致计算机故障或瘫痪，因此提高计算机的防病毒能力是提高计算机网络安全性的重要途径，计算机用户抵御病毒的能力通过安装防病毒软件改进，例如，一个计算机用户在自己的计算机上安装了杀毒软件，并定期在自己的计算机上杀毒，

同时下载支持组件，彻底扫描自己的电脑，自动发现并纠正系统中的漏洞，加强计算机的防火墙，并通过定期杀死和检测新文件，将中病毒的可能性降至最低，计算机用户可以使用市场上所有类型的杀毒软件，定期检测消灭病毒。近年来，我国网络安全部门清除了大量网络不良信息，及时纠正了一些传播不良信息的网络公司，其中一些含有网络病毒，一旦下载了这些不良信息，会导致计算机设备中的重要数据被盗，因此，在网络上下载一些未知的文件信息时，使用防病毒软件对这些信息处理，以确保下载的文件信息中不会隐藏病毒，确保计算机数据的安全，若电脑存在漏洞，应及时下载补丁，避免一些隐藏在电脑中的病毒软件给电脑造成更大损失，损害用户的操作体验。

3.4 升级杀毒软件

杀毒软件也是计算机网络安全防护中极为重要的组成部分，其可以对防火墙的不足之处有效的补充与完善，在双方结合之下，实现对计算机系统的最大限度的保障工作[4]。如今的杀毒软件已经不再局限于对病毒的监视与扫描，还能在一定程度上恢复数据。网络流量监控及控制等功能，从而降低计算机系统被病毒控制几率的同时，对计算机内部文件最大化保护。而对杀毒软件升级主要还为应对如今更新速度越来越快的计算机病毒，若病毒更新了以后杀毒软件还得不到更新，就可能会造成防护漏洞，进而造成计算机系统存在安全风险。

3.5 加强风险的管控

除了在宏观层面健全计算机信息管理技术的管理机制，还需要在微观层面加强网络环境的风险管控。众所周知，用户在使用计算机娱乐或者工作时，会面临很多未知的风险，例如窃听、盗取数据、信息泄露、破坏系统和电脑故障等问题，而最常见的就是手机或者电脑被植入木马或者病毒。面对这些破坏网络的风险，必须多层次的全面防控，降低风险问题的出现频率，促进网络环境的净化和安全。

有关部门要构建一个更加严格的防范体系，避免出现不必要的网络安全事故。具体说来，就是要在网络中安装相应的预警系统或者预报系统，对网站中可能出现的恶意信息提醒和拦截，提高信息访问的控制效果，防止用户进入携带病毒的网站或者使用相应的软件。另外，面对可能到来的网络安全事故，要提前做好规划，提高应对风险的能力；

用户本身也应养成网络安全防护意识，自我管理和控制网络中的言行举止[5]。不要随意点击无关的广告或者链接，充分认识网络风险的类别、原因和应对手段。

3.6 充分使用计算机网络的杀毒软件

实际上，绝大多数的计算机会在安装过程中配备一定的杀毒软件。通过安装杀毒软件，在一定程度上可以更好的提高计算机对于垃圾信息的自身防御能力。而将防火墙技术与杀毒软件有效的结合起来，能更好的对计算机网络运行过程中可能会存在的威胁排除，将安全性能提到最高。现阶段，日常使用的杀毒软件有腾讯管家、电脑管家等，市面上的这些杀毒软件均能达到日常保护计算机网络信息安全的基本要求，但在使用过程中应注意，每台计算只能安装并运行一个杀毒软件，这是为避免产生系统冲突。此外，为提高杀毒软件的使用效果，相应的计算机使用人员也应提高计算机信息安全保护的意识，并且对杀毒软件及时的更新处理，将垃圾信息最大限度排列在计算机网络系统之外。信息资源重要的企业机构需要充分的考虑自身发展情况来提高计算机的安全系数，尽可能地使用对应的数据认证技术，在一定程度上提高访问计算机的门槛，为企业前进发展提供强有力的技术支持[1]。

**结束语**

随着计算机网络技术的普遍应用，网络安全隐患也就会产生，一般用户大多只能采用相应的网络安全软件以及对防火墙设置和数据加密等方式来确保安全使用网络。软件设计人员则需要强化对相关软件，尤其是智能设备上的安全软件，研发和及时的升级，从而有效的从整体上实现网络安全防护水平的不断提升。

**参考文献**

[1]刘思琪，穆莉.计算机信息网络安全技术和安全防范措施探讨[J].科技风，2020（09）：101.

[2]李锦慧.计算机网络安全技术与防范措施[J].中国新通信，2020，22（02）：146.

[3]姜伟.计算机网络安全技术与防范措施探讨[J].信息与电脑（理论版），2019，31（24）：185-186.

[4]李义.计算机网络安全技术与防范措施[J].科技风，2019（25）：94.

[5]明志.浅谈计算机信息网络安全保护策略与关键技术[J].网络安全技术与应用,2018,12:12+31.