计算机网络安全及其防范措施探究

周 庆 李 琳 卢 镭
江西应用技术职业学院，中国·江西 赣州 341000

【摘 要】当前，计算机技术已经渗透至我们生活的方方面面，对于社会运行模式都有着直接的影响和改变，但在网络时代，有关计算机网络安全的问题频频发生，个人信息泄漏、各种网络攻击等等，都对计算机安全造成了很大影响。计算机网络安全实质上就是使计算机系统始终处于安全稳定运行状态，并且对计算机系统内所有信息数据都给予有效保护，使其免受恶意泄漏或攻击。在此背景下，人们愈加重视计算机网络安全的技术研发和防范。本文从计算机网络安全与防范措施方面进行了相关探讨。

【关键词】计算机；网络安全；综述；问题；措施

近几年来，我国计算机网络技术一直处于快速发展通道，以大数据、云计算、5G 通信、互联网等技术为代表的信息化技术得到了极大发展，使得我国经济社会有了很大进步。当前，我国计算机网络技术水平稳居世界第一梯队，在国际竞争中占据有利形势。但是在实际运行过程中，计算机也面临着较为严重的网络安全问题，其中尤以信息泄漏问题与网络攻击问题最为严重，因此，如何有效解决这些问题，构建起一个安全的计算机网络体系，成为当前人们重点关注的对象。

1 计算机网络安全综述

目前，计算机网络安全是指采取特定技术或管理措施来保障计算机运行安全。也就是说在计算机运行时，不管是硬件设备或者软件信息都能够得到有效保护，不被破坏、窃取和篡改，使计算机网络得以稳定安全运行。

1.1 信息安全

数据信息是最重要的网络资源，也是计算机网络安全核心所在。网课、云办公等新型学习、工作模式已然成为计算机主流，在网络上每分每秒都在产生海量数据信息。有统计数据表明，2016 年一分钟内人们就能够通过网络发送 1.5 亿份邮件、完成 240 万次搜索以及数以百万的账户登录，这些数据都足以证明当前计算机网络已经处于信息大爆炸的状态，并且趋于常态化。与之相对应的就是信息安全问题也频频发生，许多不法分子利用各种违规手段强行破解、阅读和更改互联网用户信息以及企业内部信息，导致信息泄露事件层出不穷，成为当前信息安全防护工作重中之重[1]。

1.2 网络安全

现阶段，作为计算机网络安全终端服务对象，网络安全针对网络数据私密性和完整性特征，利用计算机技术强化和网络安全管理升级来实现上网环境的安全。网络安全内容繁杂，包括系统因素、网络因素、管理因素、应用因素以及物理因素等多个方面。网络平台自身开放性特征注定难以有效筛选网络接入者，加上网络环境经常处于难以控制状态，加上黑客群体活动等等因素影响，使得网络安全问题日益严重。同时，为满足广大用户自身需求，需要对计算机系统进行定期不定期的升级，而复杂化、多元化的系统升级会带来安全漏洞增加的风险，也就降低了网络安全保障性。

2 计算机网络安全常见问题

2.1 计算机系统安全问题

当前计算机系统安全问题属于常见计算机网络安全问题，大致可以分为硬件问题与软件问题，硬件问题针对的是计算机配置上存在的安全隐患，硬件配置如果出现问题将会对计算机正常使用及稳定运行造成直接影响，还有可能导致信息数据丢失。软件系统问题主要是指计算机数据库或操作系统存在一定问题，这些问题如果没有得到有效解决将使数据库安全性直线下降。究其原因，主要是一些网络用户自身安全意识淡薄，在数据信息管理上重视程度不足，对于计算机安全漏洞管理上缺少经验，使得计算机网络系统很容易受到外界破坏或侵袭，从而引发一系列安全问题。尤其是为满足当前社会发展需求，许多企业自行编写软件优化系统性能，促使操作更加便捷，但是开放型操作系统的源代码是对外公开的，在开源协议指导下，个人或企业都能够进行优化编译及二次分布，由于不同企业自身计算机水平存在差异，很容易产生系统维护困难以及软件兼容性不够等问题，也会影响到计算机网络安全性[2]。

2.2 网络病毒侵袭

计算机安全隐患中，最具破坏性的当属计算机网络病毒。其可以通过光盘、U 盘、硬盘等多种储存介质或网页，在计算机开启后爆发复制性与传染性非常强的病毒，攻击整个计算机系统，导致计算机无法正常运作，甚至会使计算机系统崩溃，出现蓝屏或黑屏现象，更为严重的是会引发计算机内部信息资料及数据文件丢失问题，比如企业招投标文件的竞标信息一旦被竞争对手所获取，将会造成巨大经济损失。

2.3 黑客攻击

黑客指的是信息安全领域当中专门研究与破解计算机系统安全的人员，这类人员精通计算机操作、熟悉计算机系统各种漏洞、擅长设备维护，特别善于破解用户密码入侵他人计算机，从其本质上来说属于违法行为。黑客入侵的主要目的是为了查看他人计算机中重要数据信息，甚至对其进行恶意篡改，然后将这些数据信息对外售卖以谋取非法利益。近些年来，黑客进行网络攻击频次越来越高，给企业或个人用户带来极大威胁，系统被黑客攻击过以后，轻则受到黑客控制，重则导致系统瘫痪，引发一系列严重后果。

3 计算机网络安全有效防护措施

3.1 强化网络系统安全管理

要加强开放性操作系统管理，加强安全防护。可以通过文件加密、加强目录和文件访问许可等方式加强系统安全防护，这样不但可以保留系统编写自由，而且能够增强私密性。要加强网络安全防范意识宣传，充分利用传统媒体和新媒体相结合的形式，在网民心中牢固树立起安全防范意识。

网络用户要规范自身行为，养成定期清理系统的良好习惯，有效防范开放性操作系统带来的安全问题。要养成设置登录密码的习惯，而且密码设置不能够过于简单，促使计算机使用安全性。对于计算机中一些重要内容也要实行加密设置，最好做到定期更

换密码，降低计算机被入侵几率。对于来源不明的网页链接，一定要提高警惕，网络用户要减少在公共场所登录个人账户，尽量保证个人账户安全，如果计算机受到非法入侵或者病毒攻击时，要及时举报，扎实履行好网民社会责任，切实维护网络安全。要做好访问权限设置，通过IP地址或用户口令等方式进行设置，未经授权不允许访问，另外，计算机系统管理人员需要将进入口令定期更换，关闭无用服务器端口，保障计算机网络系统安全[3]。

要树立正确网络安全意识。针对系统漏洞问题，相关程序设计人员在系统设计时要尽量做到完善，加强系统更新，确保系统能够满足广大网络用户需求。针对操作人员自身失误问题，要不断加强网络用户自身网络安全意识。对于网络用户忽视网络安全现象，有关程序设计人员可以设计相关程序来进行提醒，比如建立定时提醒系统加强网络用户安全意识。利用常规提醒（以三天至七天为一个周期）形式，让网络用户对计算机系统定期进行检查，筛查剔除无关紧要的数据信息，使计算机系统内部数据得以简化，还可以及时察觉计算机系统存在的安全隐患，并进行应急处置。

3.2 安装安全防护软件

为有效提升计算机安全性能，网络用户需要不断提升安全操作意识，采取安装防火墙、防护软件等有效措施来保护计算机数据信息安全。一旦出现病毒入侵现象，防火墙会在第一时间进行过滤与拦截，同时对网络用户使用的网络进行监测保护。安装安全防护软件的目的是对计算机系统内部有可能存在的病毒开展监测，利用实时提醒方式来提醒网络用户加强防范，一旦有病毒或恶意入侵木马出现时，可以直接以弹窗形式提醒用户，做好安全问题排查工作，及时处理突发病毒，以免计算机数据信息遭受盗取或破坏，确保计算机安全。要对杀毒软件进行及时更新，高度重视杀毒软件研发和维护，并进行持续更新升级，以适应病毒发展。当前计算机硬件设施更新换代极快，各类软件也一直处于优化性能状态，但是新系统发布后，一旦有漏洞就会遭到各种攻击，这时候开发者经常会发布各种各样的安装补丁，以保障系统安全，因此，必须及时安装系统漏洞补丁，确保计算机系统安全。

3.3 从技术层面做好计算机网络安全防范

定期对服务器日志进行检查，管理密码要不断更新，如果具备较强代码基础可以注入安全代码进行相关控制，对计算机进行不定期安全扫描，充分利用第三方免费扫描服务。另外，还可以接入第三方云安全服务，使用隐藏IP地址的方法防止黑客攻击。对于个人重要数据如信用卡、密码等，在服务器和客户端之间进行传送时应当经过加密处理后再予以发送，这样就可以有效规避黑客监听和截获。在加密选择时应当选择破解不易的加密方法，比如DES加密模式，该加密算法没有逆向破解方式，黑客遇到这种加密文件时，只能够采取暴力破解方式。

还可以通过安全扫描工具来防止黑客入侵，做到安全检测常态化，强化内部网络和系统安全防护，及时发现安全漏洞，查找薄弱环节，提升系统抗破坏能力，如果网络或者系统受到黑客攻击时，扫描工具可以及时找出黑客入侵痕迹，进行有针对性的处理。系统管理员要养成定期备份的良好习惯，以便受到黑客攻击时可以及时修复，最大限度减少损失[4]。

3.4 其他安全技术

计算机网络安全技术需要做到制度管理严格化、标准化、规范化，重点做好以下几个方面的工作：一是网络信息匿名化。由于计算机网络在使用过程中涉及大量用户隐私，对用户来说，这些隐私信息极为重要，这也是计算机网络安全管理的重点内容。网络信息数据匿名化能够起到有效保护，当前常用的匿名保护方式有点匿名与边匿名两种，点匿名实质上就是在信息发布时就将用户信息进行隐藏，边匿名则是在信息发布时隐藏用户之间的关系。二是网络信息水印化。信息水印化主要用于版权保护，数字水印技术起初运用在图像上，后来扩充至声音、视频等各种数字媒体。近年来，随着关系网络数据信息库受到大众青睐，许多人又开始在其中嵌入水印信息，以保护版权和认证来源。三是网络信息跟踪溯源。所有网络信息都有其运动轨迹，利用其运动轨迹来追踪网络信息所处状态或用途，或者在网络信息发生泄漏事件后，利用运动轨迹溯源能够找出攻击对象，从而找到隐私泄漏源头所在。

网络时代，人们生活日益便利，但是也有了信息安全的烦恼，如何在网络时代保障信息安全，是当前人们亟待解决的问题，因此，很有必要制定安全可靠的应对策略，运用各种安全技术来保障计算机网络信息安全，为和谐社会构建作出贡献。

参考文献：

[1]王薇.计算机网络安全问题及其防范措施分析[J].无线互联科技,2021,18(03):37-38.

[2]李文骞.浅析计算机网络安全问题及其防范措施[J].信息记录材料,2021,22(02):65-66.

[3]刘诗鹏.浅析计算机网络安全问题及其防范措施[J].数码世界,2020(11):260-261.

[4]潘龙.计算机网络安全问题及其防范措施研究[J].数码世界,2020(09):186-187.