计算机信息系统网络安全现状及分析

李　静
阿拉善职业技术学院　内蒙古　阿拉善盟　750300

摘　要：伴随着计算机网络技术发展，网络入侵、病毒感染威胁等对计算机网络安全组成巨大威胁，导致财产损失。因而，计算机信息安全慢慢导致了大家的高度关注，可是，因为互联网信息安全种类繁多，安全防护难度高，应该根据计算机网络中信息安全隐患的种类，制定多元化的安全防范对策，搭建更安全的计算机网络环境，充分运用计算机信息技术的应用各行各业的作用。鉴于此，文中阐述了计算机网络的风险来源，并给出安全防范对策，有益于保证计算机网络环境的安全。

关键词：计算机网络；信息安全；防护策略

引言

近年来随着时代的发展，出现更为多元化的信息传播环境，伴随着各种获得信息方式的拓展，接踵而来信息安全隐患也逐步呈现。制定规范的计算机网络信息系统优化防御机制，确保信息安全散播，创建更健康相对稳定的信息传播环境，呈现大量时期价值表现，推动社会发展协调发展，起着至关重要的作用。

1 计算机网络信息安全所具有的特性

在计算机中技术的发展中，会存在一些安全风险，因而我们要采取有效措施维护应用系统的安全。网络信息安全具有一定的特点，包含硬件与软件的信息维护特性，及其计算机对应的网络安全体系，确保计算机信息系统的不断、靠谱、正常运转。网络信息安全主要有以下特点，包含安全保密性、易用性、可控性、完好性、预警信息等性能。安全就是指计算机维护其全面的硬件软件机器设备，对业务信息给予一定的安全防范措施，防止数据信息泄漏给未授权的消费者。易用性就是指关系网址可以传送和变换信息，以此来实现数据与信息资源分享。可控性就是指计算机网络系统信息散播的途径与内容具有一定的可控性。完好性就是指计算机网络系统内部信息是完备的，未授权的消费者不可修改其信息。预警信息就是指当计算机信息应用系统遭受不良软件进攻或故意侵权行为时，会有一定的自我防御机制，立即造成报案信息，从而出现客户的留意[1]。

2 计算机网络信息安全防范措施实施的重要性

2.1 有利于保护数据信息安全

就目前的高速发展情况看，计算机网络应用管理于经济发展、绿色生态、高新科技、诊疗、金融等各行各业。涉及到国家发展趋势每个方面的信息。一些犯罪分子妄图侵略盗取国家商业秘密，严重考验国家安全防范。因而，采取有效措施维护计算机网络信息安全，提高防水等级，确保数据信息安全和稳定性，有利于维护保养国家安全。确保国家纪律平稳运作。

2.2 减少信息泄漏，降低犯罪案件发生概率

计算机网络全面的运用为人们增添了便捷生产与生活，但也会带来一系列安全问题。比如，使用计算机网络系统后，一些工作人员未能及时关闭网页，同时将个人信息暴露于众人面前，一些犯罪分子借机盗取公民信息并执行网络诈骗、敲诈等刑事犯罪，严重危害公共秩序稳定和睦。因而，采取有效措施维护计算机网络信息安全，搭建安全防护网，有益于降低刑事案件产生，合理维护保养社会安定[2]。

3 计算机信息系统安全现状

3.1 个人信息泄漏风险

个人信息网络信息安全与每一个人密不可分。在信息系统内，客户个人信息保存在电脑里面。网络黑客一般运用计算机软件的开放性与传递性，运用设备或互联网的系统漏洞，侵略个人计算机盗取私人信息，再将盗取个人的信息售卖，获得非法利润。当公司或者个人信息被盗取后，很有可能会有一些严重后果，乃至是非常大的损害。拒绝服务攻击也会导致计算机网络崩溃，全部数据与信息会彻底消退。许多人在操作电脑时，个人信息时会泄漏，这会对客户导致了影响个人隐私和信息安全。信息泄漏除开黑客攻击计算机软件，也包括应用光存储或移动存储设备媒介的时候被网络黑客拷贝，造成个人信息曝露等状况。

3.2 环境危害引发的安全问题

从具体情况看，计算机网络信息系统依然存在当然以及社会环境造成安全问题。一方面是生态环境伤害产生安全问题。一般情况下，生态环境对计算机网络信息

系统优化的危害性主要来源于于水灾、火灾事故、地震灾害等洪涝灾害。这种洪涝灾害伤害覆盖面广，毁坏水平大，对计算机网络信息系统的安全伤害较大。另一方面是社会污染环境产生安全问题。社会发展伤害主要包含人为因素伤害，如人为损坏。

3.3 信息资源共享带来的安全问题

信息资源整合共享是用户使用计算机网络信息系统向别人传送已经有数据信息的信息传递过程。在这过程中，计算机网络信息系统的安全至关重要，它关系着客户信息资源能不能成功传送，客户信息资源有没有被泄漏。因而，必须提升计算机网络信息全面的安全建设。可是却现阶段的具体运作来说，计算机网络信息系统分享信息资源可能带来一些安全隐患，如资源泄漏等，会给消费者或单位导致利润损害。计算机信息系统给人们带来了方便快捷的信息共享平台，大家仅需根据此系统就能实现跨区域传送，方便了大家的生活和工作。但是，当客户跨地域共享时，导致系统安全级别基本建设不足健全，非常容易为犯罪分子带来机会，进而提升信息分享风险性的几率，最后导致客户资源失窃减少客户使用体验[3]。

3.4 受人为因素的影响

计算机网络信息安全出现安全隐患也受到了人为因素条件的限制。人为要素可将其分成下列两大类，第一类是一些软件程序员为了能维护成本工作中更加方便快捷，一般会选用设定“后门”的形式对程序执行编写，而这一编程方式非常容易被犯罪分子侵略，进而盗取所需的信息，造成数据信息泄漏，给人们生产制造带来很严重的不良影响。另一类是客户使用计算机网络系统时，因为自身安全防范意识淡薄，欠缺对应的计算机网络信息安全防护知识与技能，应用结束之后未能及时并对网页页面开展关掉，造成信息泄漏，进而为个人、企业、国家经济发展产生众多不良影响。除此之外，一部分机关事业单位并没有对办公室系统开展数据加密，一切工作人员都可以用办公用品登录网络系统，加强了数据信息泄露风险性。

4 计算机网络信息安全的防护策略

4.1 安装正版杀毒软件及防火墙

在计算机中系统的运行中，防火墙可立即、清晰地检测到互联网外界、外部环境所存有的恶意攻击个人行为，虽然对于这种恶意攻击的识别阻拦十分有限，但却无法完全处理系统的系统漏洞，针对系统自身的系统漏洞，可组装专门电脑杀毒软件，运用此软件不但可以提高系统安全系数，还能够阻拦网络黑客的出现异常侵略，对病毒攻击和木马病毒攻击操纵很有效。因而，为提升计算机网络信息安全，客户在计算机的使用的过程当中，一定要开展电脑杀毒软件安装，并立即开展漏洞修复的升级，按时开展病毒感染扫描仪。计算机网络系统里的防火墙，事实上当做是指入口的安全保卫系统，可以对进入系统中的每个因素开展安全大检查。防火墙配置，促使不一样互联网中间可以实现密钥管理，可及早发现外界非法行为进到内部网络的举动，经过外部环境的防护，可有效控制资源和内部环境。计算机网络系统里的防火墙配备，能够有效将不安全的信息过虑出来，确保系统安全系数。经过科学合理的防火墙组装，防火墙就可以从计算机网络系统中即时监管、数据记录统计分析客户浏览的现象，一旦发现了当中存有异常浏览个人行为，防火墙便会马上在系统页面上传出警示信息，提示相关负责人留意，在短时间内降低安全隐患，修复系统的正常运行。目前的防火墙技术中，包滤型防火墙、代理商型防火墙、监管型防火墙、网络地址转换防火墙的应用会比较多，具体的选用哪一种的防火墙技术，还要融合计算机网络系统的特征来挑选[4]。

4.2 注重日常计算机信息系统漏洞的检测并具备基本的入侵检测技术

高度重视计算机信息系统的安全系数，组装可监测并修复漏洞的系统手机软件，提升计算机对病毒攻击和网站漏洞扫描的预防基本功能。在其中，最重要的是必须计算机的使用工作人员要具有最基本的病毒感染防火墙技术。恰当鉴别侵略到计算机安全预警，为了能第一时间修补计算机存有的病毒感染、系统漏洞，使计算机信息系统得到充分有效的维护实际操作。

4.3 将生物识别技术和数字签名技术相结合

开展多重身份鉴别验证。伴随着科技进步水准的发展，针对互联网信息安全生产方面也在逐渐催生出更具有新科技水平的预防措施。在其中利用人体原有生物学特性去进行识别方式方法早已应用于一些关键安全防护的业务领域。这儿所称的生物识别主要通过运用指纹验证、手掌心代数学鉴别、签字鉴别、人脸识别等身体无法复制的特点去完成身份认证工作，其技术的特点相比传统的认证技术具备强劲的优点。而数字签名技术的应用，是由信息发布者所产生的不能虚假的数字串，去进行身份认证的一种合理方法。在其中包含的非对称加密密匙加密算法和数字摘要技术的发展，促使这种检验方法更具有不能赖账性，很大的保障了计算机网络信息系统安全防护问题。

4.4 充分利用防火墙等防护装置

为确保计算机网络信息安全，必须对计算机病毒能够侵略的app开展预测分析，并高效地阻拦故意侵略的app、编码、程序流程等，因而，计算机网络信息安保人员能够组装防火墙设备。根据完备的网络安全系统高效地维护信息安全，预防病毒的侵犯。与此同时，将防火墙等设备放置在计算机系统具体内容，有益于运用科技进步对系统内不正常服务器进行寻找，进而提升计算机系统内控管理指数，自然，还可以对外界信息和公共网络等进行合理防护，避免犯罪分子对它进行联接，减少病毒攻击风险性，为计算机网络信息系统安全运营服务保障[5]。

4.5 打造网络系统安全监控防范模式

在计算机中信息管理方法的大力支持下，打造出整体性互联网系统安防监控预防方式，运用大数据技术，依据电脑设备运作步骤，从便利性和安全系数等多个方面考虑，提升互联网系统运作安全系数。依据计算机网络系统版本号展开科学合理区划，在加强安防监控工作过程中，采用多样化管理方法。对于恶意攻击情况的发生，及时鉴定危险等级，接着向系统推送报警系统。安防监控预防方式的打造出，从各方面对网络安全预防水平开展提高，而且提升计算机信息管理品质。

4.6 科学开展网络安全系统风险评估

计算机信息管理方法运用到网络安全管理方面，根据风险评价的形式，合理清查网络安全隐患，而且制定相对应的防止对策。网络安全系统风险评价首先要以辨别的形式，对网络安全安全事故加以分析。其次对于网络安全风险性开展级别管理方法，而且依据实际的危害去提升网络安全防护层级。网络安全系统风险评价一定要做到整体性、精确性与目的性，及早发现网络安全系统中隐藏难题，同时对可能导致的危害性开展鉴定。分阶段对网络安全管理方法展开调节，那样才能确保网络安全健康运作，从根本上解决计算机网络安全隐患，保持计算机网络系统正常的运行状态。

4.7 加强计算机信息系统自身防护功能

在计算机中信息系统安全防护中，一般采用这两种技术来扫描仪系统漏洞，各是借助互联网的线上扫描技术和根据计算机系统专用软件的扫描技术。这几种技术可以有效完成远程控制和当地对计算机信息系统的监管。防病毒软件技术能通过不断更新病毒特征库来合理保护计算机信息系统的网络安全，避免网络病毒损害系统及数据信息。防病毒软件技术能够实时监控系统、清除、升级修复病毒感染破损的数据信息。为保护计算机信息系统，一定要做好数据库系统日常安全防范。数据库是计算机信息系统存放数据信息的媒介，为顾客在计算机中系统中获取信息，数据信息的有效控制是由形式多样达到的，如提升合理合法客户的标志识别、提升高等级的动态口令，给消费者要求不同类型的管理权限，使之不可以随意浏览不应该浏览的数据区，对信息进行数据加密管理等。应认真落实信息维护，保证计算机信息系统网络安全。要提高管理者的业务能力和综合素质能力，搞好安全维护。需要对管理人员进行必要的学习培训，提高技术以及认知水平。要经常机构专业技术人员进行系统考评，真正将网络信息安全工作做到位[6]。

结束语

总的来说，伴随互联网时代的来临，计算机网络信息系统安全建设尤为重要，其关乎着大家信息安全系数，是许多人安心使用计算机网络信息系统关键确保。因而，有关专业技术人员要高度重视计算机网络信息系统安全建设，应用优秀加密技术和网络攻防技术，提升互联网信息系统安全系数，提高大家互联网使用感受。因为文章内容篇数限定，文中有关计算机网络信息系统安全隐患及解决对策等方面的科学研究不够全方位、深层次，将来环节理应密切关注相关计算机网络信息系统安全隐患及防范措施等方面的科学研究，不断完善科学研究工作经验，以填补文中研究不足。

参考文献

[1]王毓.关于计算机网络信息安全及防护策略探究[J].科技风，2019（5）：52-53.

[2]陈晓伟.关于计算机网络信息安全及防护策略探究[J].数码世界，2019（3）：19-20.

[3]邓光芒.计算机网络信息安全问题与防范策略研究[J].科学与信息化,2020(15):36-37.

[4]杨品芳.计算机网络信息安全防护策略及评估算法研究[J].现代信息科技,2020,4(8):140-141+144.

[5]陈璐.试析大数据时代的计算机网络安全及防范策略[J].数字技术与应用,2020,38(7):193-195.

[6]丘雪.浅析影响计算机网络信息安全的因素及防范措施[J].电脑迷，2019（02）：26-27.