计算机信息系统网络安全现状及分析

苏东楠　孔凯薇　吴　斌
北京计算机技术及应用研究所　北京　100854

摘　要：随着信息化时代的飞速发展，各类计算机信息系统已广泛应用于人们的工作与生活。与此同时，由于计算机信息系统利用网络传输信息与数据，也带来了诸多网络安全方面的问题。为了做好信息系统网络安全防护措施，减少网络安全隐患，本文分析了计算机信息系统安全现状，指出了网络安全技术应用于计算机信息系统的意义，提出了确保计算机信息系统安全的有效措施。为全面提升计算机信息系统网络的安全性，加强计算机信息系统网络维护管理，提升计算机信息安全水平提供理论参考。

关键词：信息系统；网络安全；有效措施

引言

计算机信息技术的出现给人们的生产生活带来了巨大便捷性的同时，也带来了巨大的网络安全威胁，开放的网络环境下，为保障正常的网络通信，抵御病毒入侵、黑客攻击，就需要从多个角度来开展网络安全防护。随着人们对网络安全关注度的日渐提高，我国的计算机网络安全技术取得了一定的发展成效。越来越多领域在计算机信息技术应用的同时，也采用了网络安全技术，有效提高了计算机网络安全性。但因为网络环境的复杂多变性，未来还需加大在计算机网络信息安全技术方面的研究。

1 计算机信息系统安全现状

1.1 个人信息泄漏风险

个人信息互联网的安全关系着每一个人的权益。在信息系统中，用户个人的信息储存在计算机中内部结构。网络黑客一般借助计算机系统的开放式和传递性，运用系统和互联网的系统漏洞，入侵私电子计算机，盗取个人隐私信息，随后售卖并盗取这种本人信息以获得非法利益。企业或个人信息失窃后，很有可能会有一些严重后果，或是导致极大损失。拒绝服务攻击造成计算机网络系统奔溃，全部数据与信息彻底消退。除开黑客攻击电子计算机系统并盗取信息外，应用光存储和移动存储设备媒介所进行的黑客入侵也可能造成信息泄漏。

1.2 黑客入侵问题

有关计算机网络侵入难题通常是不法分子利用方式方法盗取和毁坏信息和信息以获得更多的信息。用不同的办法获得对应的信息，也会产生不同类型的结论，对计算机网络的信息安全性产生一定的危害。因而，必须对目前软件平台开展改善和改革创新。一些网络黑客受犯罪分子的诱发，从业更多违法犯罪活动，根据进攻电子计算机信息系统危害别人权益。因此目前，网络黑客成为了大家当心的一类人。网络黑客根据系统漏洞浏览计算机，盗取并毁坏计算机信息和信息。给用户导致相对应损失，有关攻击方式就会直接分裂计算机网络系统。中所有数据与信息将彻底消退[1]。

1.3 信息资源共享带来的安全问题

信息共享资源是用户根据计算机网络信息系统向别人传送目前数据信息信息的信息传递过程。在这过程中，计算机网络信息系统安全性是十分重要的。在协调器成功与否接受信息网络资源的前提下，用户信息网络资源在传送环节中是不是不被未经授权用户盗取。因而，必须提升计算机网络信息系统的安全建设。可是却现阶段的具体应用来说，计算机网络信息系统分享信息网络资源很有可能会引发网络资源外流等安全隐患，给用户与企业产生收益损害。电子计算机信息系统给人们带来了方便快捷的信息共享平台，大家能通过该系统完成信息的区域间传送，大大的便捷大家生活和工作。可是，当用户跨区域资源共享时，因为系统安全标准不足健全，非常容易为犯罪分子带来机会，增强了信息泄漏风险性的几率，进而导致用户网络资源失窃，利益受损。

1.4 计算机病毒的影响

在计算机中信息安全威胁中，计算机病毒是导致严重危害风险。计算机病毒品种繁多，体现为记忆能力、可操作性和隐秘性。因为这一特点，计算机网络一旦遇到病毒攻击，会带来很大的伤害。近些年，在我国互联网信息技术性迅速发展，市场中出现各种各样软件信息系统，也使计算机病毒入侵在其中。首先，计算机病毒隐秘性强，用户在实施电子计算机APP应用中难以及早发现计算机病毒。病毒攻击电子计算机APP程序后，电子计算机系统很有可能不能正常工作中，可能会导致电子

计算机系统错乱或奔溃。其次，当计算机语言遭受病毒侵入和伤害时，当程序流程再次运行中，计算机病毒因其潜伏性、毁灭性和传染性的特征，慢慢扩张对电子计算机系统攻击范畴。最后，病毒感染能通过电脑磁盘、光盘等进一步感染。一些计算机病毒具备强悍的拷贝水平，这类多种拷贝会大幅度降低电子计算机系统的使用效率[2]。

1.5 防护级别相对较低

电子计算机信息系统的安全标准关系着计算机网络的信息安全水平。当安全级别比较低时，不良编程代码和命令凭借强悍的拷贝能力在计算机网络系统中掩藏生存，被趁机繁殖，严重影响到计算机设备系统稳定运作。除此之外，一些机关事业单位欠缺更专业的计算机人才，互联网防病毒技术性较低，欠缺全方位的防病毒手机软件，促使电子计算机信息系统的网络信息安全严重困难。

2 网络安全技术应用于计算机信息系统的意义

做为电子计算机信息系统维护的重要构成部分，网络信息安全技术的发展是必然趋势，从微观和宏观两方面都显现出无可替代的优点。从微观来看，它不但能确保电子计算机信息系统运作和数据处理方法效率，确保电子计算机信息系统的工作效能，并且可以降低系统运作和运行维护难度。从宏观来看，信息安全技术与国家发展、信息管理方法、企业效益息息相关。所以必须提升和高度重视信息安全技术在计算机中信息系统中的运用[3]。

3 计算机信息系统的网络安全保障措施

3.1 用户身份认证

用户验证是电子计算机信息系统第一扇门是控制违法用户侵入电子计算机信息系统的最基本对策在用户申请注册环节，用特定标识外键约束标识用户信息，在系统整个的生命期中确保用户外键约束的一致性和唯一性。在登陆环节，用户的登陆个人行为需要通过登陆密码拓展操纵进行监管。假如系统不成功强制注销，或是用户登陆账号没多久没有实际操作，则用户务必再次输入支付密码才可以重登。为了确保认证安全保密性和完好性，登陆密码的存放和传送根据数据加密体制进行修复，限制登录次数和故意登陆。假如同一账号持续数次登录失败，往往会自动锁定该账号。除此之外，登陆密码要符合下列规定，才能实现登陆密码增强效果：(1)限定最少密码长度，登陆密码及时更新，不可多次重复使用同一登陆密码。(2)规定登陆密码的多元性时，强烈推荐标记、字母和数字的组合方式。(3)初次登陆账号时，务必改动系统默认设置账号账号和密码。用户无法使用初始密码。(4)假如系统不兼容以上设置密码规定，能够减少拆换时长，但请应用系统鼓励的最多登陆密码。(5)电子计算机信息系统也可采用一次性密码验证)[4]。

3.2 黑客防御相关技术

为了避免黑客攻击，务必首先运用入侵检测技术以加强内部结构用户的访问限制。网络防火墙技术的发展已经完善，市场中有关的开发软件还在健全。比如，现阶段用户广泛应用的360安全卫士防范是入侵检测技术的营运商。

其次，使用了防火墙技术。因为一部分计算机网络进攻具备隐秘性，能通过防火墙技术改善现阶段计算机网络安全生产技术的风险评估系统。入侵防御系统具备实用性的特征，能通过电子计算机的内部安全隐患检验立即提示用户。与以上计算机网络安全生产技术不一样，防火墙技术具有一定的自觉性。防火墙技术的工作方式可分为异常检测和错用检验。不一样的检查方式能够用于不同种类的电子计算机信息系统。最先，出现异常检测精度比较高，但实践应用环节中，欠缺全方位的恶意攻击检测能力。关键方式有贝叶斯估计、贝叶斯网络检测、实体模型可能、机器学习算法等。误用检测在实际操作的过程中，对异常风险的检查较为敏锐，但整体的漏报率较高。主要的方法有模式匹配法、专家系统法等。有关工作人员可以根据计算机网络的实际需求，进行入侵检测工作模式的选择。

网络黑客防御力需也要网络检测技术。安全扫描技术的重要原理是运用计算机设备监控计算机。在漫长的执行过程中，网络检测技术催生出下列四种关键技术形态：好用监管信息技术、电子计算机监管信息技术、总体目标易损性监管信息技术以及计算机网络监控技术。现相关负责人可以根据电子计算机不一样位置信息泄漏状况采用不同类型的网络检测工程措施[5]。

3.3 网络防火墙技术

网络防火墙做为保护计算机网络信息安全的重要途径，是受法律保护网络和外部网络间的天然屏障。在维护环节中，网络防火墙根据合理监管捕捉的信息具体内容并限定一部分捕捉具体内容，进一步维护内网信息内容免遭偷盗、伪造和恶意攻击。网络防火墙做为外部网络和网络信息安全域间的网关的出入口，运用智能化安全设置控制与管理间的信息流，高效地抵挡进攻。网络防火墙除开维护信息安全性外，还能够监管、控制与管理方法内部网主题活动，增强了内部网信息的内容安全防护，很好地推动了电子计算机信息系统的安全操作。

3.4 完善计算机信息系统

因为电子计算机信息系统上存在系统漏洞，网络黑客和不法分子可以借助其缺点入侵别人的电子计算机系统，根据技术性系统漏洞盗取用户数据信息，获得非法利润。所以必须立即提升和优化电子计算机信息系统以确保电子计算机信息系统的安全。立即提升电子计算机信息系统升级能够降低系统的易损性和防御力。与此同时要充分调动计算机系统维护机器设备功能的，提升电子计算机信息系统的适应能力，保证电子计算机信息系统的安全。用户必须创建一定的归属感，确保用户名和密码设定的繁杂安全度，还能够运用根据特点的验证方式进一步降低安全隐患。除此之外，电子计算机信息系统融合防无线电波泄漏、文档加密、防违法硬件配置浏览等系统维护技术，可以有效的保护计算机信息系统免遭源的影响。

3.5 传输加密与存储加密技术

传输加密、存储加密技术是电子计算机信息管理方法不可或缺的一部分。在具体APP运用中，加密技术性主要包括二种加密处理措施。一个是端对端，另一个是路线加密。端对端加密就是指发送方对信息开展加密，转化成数据文件，随后发送至信息接受方。在过程中，非接受端口号识别不了数据信息。当缩小分类被推送时，系统马上编解码该分类并把压缩格式转化成可识别文件格式。路线加密要在密匙的支持下所进行的，能够防止路线在传输数据环节中受到伤害或危害。从信息维护方面来讲，路线加密安全性更高一些，不会对源造成极大的冲击性。加密还涉及到二种处理办法：密钥管理和保密操纵。密钥管理就是指用户浏览信息时，应用对登录权限的控制与审批，避免储存的信息被违法用户盗取，确保操控的合理合法。保密操纵指的是对被存放的信息开展加密，在多种加密控制下确保信息安全性[6]。

3.6 隐藏IP地址

不法分子一般根据网络监测技术获得用户信息，并从而获得用户IP地址。犯罪分子获得用户的IP地址后，跨站脚本攻击进攻和拒绝服务式攻击能够危害用户对电子计算机信息系统的浏览。因而，掩藏IP地址是保障用户安全有效途径。IP掩藏主要指避免不法分子根据服务器代理获得用户的IP地址，进而避免不法分子的一系列进攻。

3.7 数据库备份恢复技术

储存电子计算机信息系统数据信息，相关专业人员理应提升备份数据保护和，与此同时应用数据加密技术，提升数据信息共享资源安全，维护用户信息。为了保护数据信息信息，避免内容丢失，有关专业技术人员应经常备份数据库具体内容。假如系统发生意外的内容丢失或泄漏等安全隐患，管理人员能够备份恢复的信息以保证信息的完好性。为了能保证数据共享资源的安全性，有关专业技术人员需要使用验证和加密密钥对信息进行加密。假如用户想资源共享，则需在身份认证成功之前寻找资源，才能实现信息共享资源流程的安全等级。

4 结束语

为了最大程度减少计算机信息系统在网络安全中带来的问题与危害，就要深入探究影响计算机网络信息安全的因素，并对症下药，找寻提高计算机信息系统网络安全性的措施。充分利用防火墙等防护装置筑牢安全防护网，增强用户安全防护意识和防护技能，提升开放型系统安全防护能力，完善计算机信息系统网络安全管理机制和测评方案，多措并举提升计算机信息系统风险防御能力，为计算机信息系统的安全运行保驾护航。

参考文献

[1]高喜桐.计算机信息管理技术在维护网络安全中的应用策略探究[J].计算机产品与流通,2019(4)：21,112.

[2]刘冬兰，刘新，张昊，等.基于大数据的网络安全态势感知及主动防御技术研究与应用[J]. 计算机测量与控制，2019，27(10)：229－233.

[3]张海悦.计算机信息管理技术在网络安全中的应用[J].中国新通信,2019,20(23)：93-94.

[4]苏文清.计算机网络信息安全及其防护措施[J]. 信息记录材料，2020，21(10)：40－41.

[5]周岩，杜健持. 高校网络安全防护中计算机信息管理技术的应用[J]. 电子技术与软件工程，2021(8)：241-242.

[6]张静. 计算机信息管理技术在网络安全应用中的研究[J]. 网络安全技术与应用，2021(3)：150-152.