

数据通信网络维护与安全问题分析

陶 嵩

长江宜昌通信管理局 湖北 宜昌 443000

摘要: 数据通信互联网在这个时代发展过程中起到不可缺少的作用,在给人们生活产生巨大便捷、提供更好的社交网络平台的前提下,正面临着众多安全隐患。数据通信网络运维是有效的确保网络安全的重要因素,必须从各方面去维护长期稳定数据通信互联网的可靠性和稳定性,进而进一步提升网络技术应用综合性,提高数据通信网络安全综合能力,为构建和谐网络安全气氛打下基础。因此掌握数据通信的作用、网络安全难题所发生的缘故,针对处理网络安全安全隐患,进行相应的管理方法拥有十分重要的作用。

关键词: 数据通信;网络维护;安全问题

引言

数据通信网络安全问题的产生会让网络系统运作的稳定、信息数据准确性与稳定性等造成不良影响,主要包含病毒攻击、软件漏洞及其系统软件不完善等,最终形成数据通信网络安全问题,不能满足各单位、企业运用及发展需要。面对这种情况,还需要关键解决数据通信网络安全问题,有针对性和根据经展开研究,制订有关解决对策。根据整体性评定网络信息安全,操控数据通信网络系统直播,再提升数据通信网络安全管理幅度,运用加密算法和防火墙技术等形式,提高总体技术实力。

1 数据通信网络维护与网络安全概述

数据通信网络都是基于一定的协议书的前提下,根据有线电视和无线等几种安全通道,对不同类型的计算机系统开展网络联接做到互换信息目的数据通信技术性。针对不同电脑设备的消费者来讲,能通过构建起的网络方式开展信息网络资源、文档等内容互换共享。在数据通信网络之中有明确归类,分类依据是网络位置和覆盖面积,种类包含国际网、局域网和局域网络,国际网是覆盖面积比较广泛的信息网络,许多人在日常生活经常使用的网络种类便是国际网,而局域网的覆盖面积窄小,一些机关事业单位通常会充分考虑内部结构信息安全性,而使用局域网络,进而在企业内部完成财务报表信息和人事部门网络资源信息的共享,此外,也对网络安全性给出了更高要求。

数据通信网络安全性主要指在数据信息网络运行的过程当中,因为人为因素或客观原因等毁坏或丢了一部分数据信息信息网络资源,最后对网络机器设备和系统造成一定的等影响不能正常运行的情况。实际上,最小网络系统软件能够归纳为服务器、传送媒介和用户终端

三个部分,在数据通信网络运行环节中,一旦这三个环节里的任何一个出现异常或难题,都会导致系统软件不能正常运行,组成一定的网络安全风险^[1]。

2 维护数据通信网络安全的意义

数据通信网络系统凭着自己的优势与作用,能够对各个领域发展趋势产生很大影响。则在应用环节,需重点关注网络安全管理与维护工作中,并采取相应维护对策,减少网络安全风险性,这样有利于对网络系统中常存放的信息数据信息合理化维护。因而积极主动开展网络安全维护工作中尤为重要,其主要目的是为了保证信息数据准确性和网络系统稳定性等。各项任务的开展既是一项技术难点,且具有社会认知和盈利性等优点。需有关部门密切关注此层面,根据数据通信网络系统具体应用状况,考虑到其安全性维护工作中经济收益,保证数据通信网络系统安全运营,为企业发展、企业等稳步发展产生积极作用。除此之外在各种信息传送数据和分享环节中,为保证信息数据准确性与安全系数,可以通过数据通信网络安全维护对策去满足公司、企业运用及未来发展规定。

互联网时代的信息信息具体内容变得越来越丰富多彩,数据信息信息的方式也多元化,比如图片与视频方式的信息信息。互联网时代的信息信息量在短期内有所增加,数据信息信息和建立模型的传输速率快速提升,数据通信互联网信息安全系数问题和日骤增^[2]。在安全防护领域,一定要考虑全面的各个领域,务必综合考虑系统设计里的系统安全性有一定影响综合要素。创建数据通信互联网维护管理系统,强化对网络病毒的安全防护,创建互联网监控系统,并且通过IPS防火墙技术维护数据通信互联网安全性。务必系统设计开展全面分析,使数据通信网络安全维护设计更为系统软件全面,从而

实现一个可靠的数据通信互联网。

3 数据通信网络维护与安全问题分析

3.1 网络安全管理工作人员安全意识淡薄

网络安全管理工作人员安全防范意识做为数据通信网络信息安全的另一关键因素,其安全防范意识的高低直接向网络信息安全造成功效。一般而言,数据通信网络系统是通过管理人员进行统一管理工作的,管理者综合性能力和专业技能的好与坏与数据通信互联网的安全性拥有紧密联系。但是,在具体的数据通信网络安全管理中,大部分管理者综合能力欠佳,实际操作不合规,管理模式老旧,对于已经的安全防范技术性没法密切关注再加以应用,对数据通信互联网安全问题增添了巨大安全隐患。

3.2 软件漏洞

移动数据网络软件漏洞难题易出现且较普遍。引起软件漏洞安全隐患的影响因素比较多,关键是在软件运用环节中,主要是因为软件类型较多并软件总数延续性提升。尽管各种软件在计算机网络中发挥了重要意义,但会带来一定安全安全隐患^[3]。目前,世界各国已对电子计算机软件制作技巧增加科学研究和创新幅度,电子计算机软件制作技巧愈来愈完善,但还会因操作步骤不合规和安全防范观念较劣等因素的影响,使电子计算机软件发生漏洞难题,给犯罪分子窃取和毁坏信息和数据提供资源优势。

3.3 计算机系统和软件机械故障

计算机系统系统软件包含运算器、控制板、储存器和输入输出设备等,这种设施是计算机软件运转的基本,在某一构件出问题的情况之下,都会导致机器设备偏瘫、没法正常运行。在当前电脑设备运行时,一般会有如下所示相关的问题:一是静电感应要素对电脑主板里的BIOS处理芯片导致浸蚀,从而使基本电源电路遭受毁坏;二是在电子计算机超时间处于超负荷工作,运行内存发生显卡超频状况导致死机和发烫比较严重的现象;三是在零配件品质不合格的情况下,促使数据和信息在传送过程中遇到遗失或者被改动。而软件层面安全隐患相对性比较隐蔽^[4],除客观原因所造成的漏洞状况以外,还会因为人为因素设计方案或是升级不到位所造成的漏洞状况,给数据信息安全导致不良影响。

3.4 病毒攻击

数据通信网络里普遍安全问题之一就是病毒攻击,其较大特征就是病毒速率很快,会到散播上对网络系统可靠性和可靠性等导致比较大水平的毁坏,没法保证网络系统安全性。与此同时,近年来随着现代信息技术迅

速发展,电脑病毒毁灭性越来越强大,病毒感染影响程度慢慢扩张,威胁计算机技能与设备运行可靠性。

4 数据通信网络维护与安全

4.1 提高网络安全观念,加强网络安全日常维护工作

在数据通信网络维护与安全防范措施工作上,提高相关负责人的网络安全观念,是保证各类安全防范工作中可以得到充分开展并执行的主要前提条件与基础,针对数据通信网络维护充分发挥具体效应起着至关重要的作用。所以在网络维护安全生产工作开展时,应先在外部搭建相对性完备的数据通信网络维护与安全防范措施管理办法和体制,针对各类网络安全防护工作中应当由专业的专业人员予以处理,避免因为外行工作人员操作失误从而影响网络安全安全防护相关工作的成功开展。次之解决参加数据通信网络维护的专业人员加强业务培训,培训计划包含网络安全维修的各种各样规范及使用关键点规定,提高专业技术人员的业务能力和专业素养,避免人为失误导致网络系统漏洞,危害网络安全^[5]。此外,解决涉及到网络安全维护保养的人员提升相关的法律法规学习培训,以相关法律法规对人员岗位职责产生牵制,标准人员的管理活动,在出现网络安全维护保养问题的时候,应及时处理并找准问题形成的原因,并且对导致问题工作人员进行相应的惩罚与处理,保证网络安全安全防护人员的坚守在管理制度前提下开展,提升数据通信网络维护相关工作的高效性。

4.2 搭建标准化的网络数据通信方式

若想合理加强数据通信网络安全性,一定要逐渐构建完备的网络数据安全法,确保网络信息提取规范性和合理化。在开展网络信息获取工作的时候,实际上也可以完成对网络信息的安全性查找。对于非结构化数据与半结构化数据文字的获取,必须先把它转变为存放方式。一般来说,人类语言文本检索方式与自然语言理解方式并没有比较大差别。

4.3 提升身份鉴别与认证技术,降低网络信息泄漏风险性

为了能进一步提高电子计算机网络信息安全性,除开一定要做好网络按时安全风险评估工作之外,还需要逐步完善身份鉴别与认证技术。身份鉴别与验证即客户或技术员在进入计算机网络的时候需要证实的真实身份信息和身份管理权限。传统身份鉴别与认证技术为“账户 登陆密码”的认证玩法,不能满足现阶段电子计算机网络安全防护的需求,因而,必须更新身份鉴别与认证技术,减少网络信息泄漏风险。比如,在公司具体运行时,主管部门除开“账户 登陆密码”的认证方式以

外,能增加生理学信息认证方式和VPN认证方式等多元化的认证对策,一起经常性地拆换认证方式,严格把关公司信息的获取权限,从根源上保证网络安全^[6]。企业能够针对不同部门或工作人员的岗位职责来决定客户或专业技术人员的应用管理权限,用户可根据自身岗位职责获得相匹配信息,防止信息获得的繁杂性。

4.4 提升网络安全潜在风险剖析

伴随着电子计算机网络科技的飞速发展和快速推广,电子计算机数据通信运行中所面临的网络风险性慢慢向着种类复杂,方式多元化的状况发展趋势,因而必须对这种隐性的威胁网络安全的潜在风险开展深入分析。尤其是在数据通信网络运行中,必须审查每个网络连接点数据信息信息信息真实性和精确性,并对这种潜在性要素很有可能带来的影响开展深入分析,采用合理的方式予以处理,确保数据信息安全性。对于一些极为重要的数据通信阶段应严格监督解决,强化对这一部分数据通信环节安全工作关键技术研究,根据集中控制系统的形式对这一环节的运行状况执行动态性监管,及早发现其存在的问题并采取有力措施进行解决^[7]。

4.5 提升网络管理方法相关负责人的技术实力

为解决我国现阶段存有的网络安全难题,重中之重是提升网络管理方法相关负责人的技术实力,仅有具有精湛的技术专业专业知识技能,才能够开展数据通信网络维护等相关工作。要高度重视专业技术人员的专业知识技能贮备,在通讯技术网络维护与电子计算机网络安全层面出现问题精确剖析,找准问题发生的缘故,并利用专业知识技能快速寻找行之有效的应对策略与对策^[8]。一方面,工作部门理应意识到塑造电子计算机人才的重要性,加强对电子计算机网络人才培养与引入幅度,采取有力措施提升网络管理者的技术实力。另一方面,主管部门需对网络管理者开展培训或调查,掌握现阶段专业技术人员的能力水平与沟通能力。与此同时,针对薄弱环节加强引导与催促,促进专业技术人员依照单位规定系统化把握通讯技术网络维护与网络安全的基本知识,进而更好的开展电子计算机网络安全安全防护。

4.6 评定数据通信网络安全指数

近些年,电子计算机网络遭遇错综复杂的进攻风险骤然增多,跨过了社会发展界限,给人们的生活、健康

与社会发展增添了很严重的经济压力,这是因为信息服务的持续增长、信息集体使用及分享所造成的。因而,在计算机中网络内进行风险评价是一个极为重要的难题。从应用统计学来看,近年来很多机构安全性能呈现了令人堪忧的态势,如网络诈骗、本人信息、数据信息盗取、网络特工活动、网络黑客或拒绝服务式攻击,很多大中型基本上都是电子计算机网络安全系统漏洞的受害者。风险评价代表着对于每一个特定事情,随后考虑到安全性的方法去达到目标,有利于掌握出任务时所涉及到的风险性,以避免损害。识别风险,首先明确风险性的源头。次之,要明确什么每日任务也会受到如何更好地受伤害。除此之外,采取有效措施规避风险做好记录与实施。最终,进行相应的查验。

结束语

总的来说,数据通信网络作为一个信息传统网络方式,各项工作开展都要创建在网络自然环境基础上,与此同时具体通信质量也和网络安全性中间拥有密切的关系。因而,为了保证数据通信网络维护实效性,一定要深层次研究和分析网络安全问题,进一步提升数据通信网络的总体安全级别。

参考文献

- [1]徐晓红,米夏.数据通信网络维护及网络安全的问题研究[J].通信电源技术,2021,38(01):180-182.
- [2]李竹申.数据通信网络维护与网络安全问题分析[J].网络安全技术与应用,2020(01):3-4.
- [3]王文静.大数据背景下信息通信网络安全管理策略研究[J].广播电视网络,2021,28(04):59-60.
- [4]朱爱龙,刘润斌.数据通信网络维护与网络安全问题的相关分析[J].信息周刊,2020(9):1.
- [5]马成果,张旂伦,诸葛绪朋.现阶段对数据通信网络维护及网络安全的相关思考[J].数字通信世界,2019(12):140.
- [6]林庆锋.关于数据通信网络维护与网络安全问题的探讨[J].现代工业经济和信息化,2020,10(08):80-81.
- [7]张士波.数据通信网络维护与网络安全问题分析[J].中国设备工程,2020(18):65-67.
- [8]郑翔.计算机数据通信网络安全维护要点探索[J].中国新通信,2020,22(20):34-35.