

# 计算机网络运维及安全管理设计探究

李 可

北京计算机技术及应用研究所 北京 100854

**摘 要：**文中首先简要介绍了计算机普遍安全隐患、网络黑客攻击、数据存储安全隐患和用户缺点，随后阐述了现阶段计算机网络运维技术的应用，文章内容强调计算机系统运行中不可避免地安全隐患问题，为了能最大程度地充分发挥计算机系统运行安全系数，应高度重视运维工作和安全生产管理的开展，应用前沿的运维管理技术，与此同时提升计算机网络运行维护的各个阶段运营维护。

**关键词：**计算机；网络运维；安全管理

## 引言

网络信息安全技术给我们的生活带来了巨大的便捷，并且也存在一定的安全隐患，必须引起重视，互联网APP网络信息安全技术具有重要价值意义。但计算机互联网运行中，依然存在安全隐患，必须引起重视，规定相关人员强化安全管理工作中。

### 1 加强计算机网络安全管理的重要性

计算机系统安全管理方法以计算机运用数据库管理为原则，对业务数据进行安全生产方面的监管。计算机应用系统的安全管理重点就是资源优化配置的易用性、完整性和安全，最后推动计算机应用系统内部结构资源优化配置的健康发展。针对计算机应用系统的安全设计，在确保互联网信息顺畅、内部结构信息资源安全的前提下，完成资源的分享，能提高具体工作效能。有关现今计算机的应用，由于使用却不标准，相关专项效率不高。日常维护管理方法计算机互联网，可以有效的提升相关工作科学性和合理化，推动计算机的使用效率，减少有关维护成本。现阶段我国全部计算机互联网的安全标准还处在发展过程，在互联网技术方面的运用还要进一步深入研究。在信息化建设过程中，想要实现网络资源运用及管理的安全指数，就必须完成对应用系统技术运用的标准化管理，这会对社会性公共服务系统的改革与创新产生一定的促进作用，具有重要实际意义<sup>[1]</sup>。

## 2 网络安全特征及运维技术探究

### 2.1 计算机网络安全特征

现阶段，计算机网络信息安全特性主要体现在以下几方面。一是安全保密性。计算机网络加密型与用户的网络信息安全息息相关，都是搭建计算机网络安全系统必须达到的关键作用之一。现阶段的计算机互联网由不同类型的硬件条件和内部网络构成，为了能高效地维护网络信息安全必须采取足够的对策。二是全面的整体

性，全面的整体性是源数据、数据类型、数据信息。三是易用性，主要指信息数据库的用户使用一系列实际操作完成网络里数据信息的获得。四是指在开展网络沟通时，信息服务提供者和信息接受者在内容与形式上保持一致，不能出现对数据信息的否认。

### 2.2 计算机网络运维技术

在现在的计算机网络运维中，广泛应用且效果较好的运维管理技术主要有三种，即风险评定技术、异构体结合技术和管理决策。

对于风险评定技术，通常采用剖析技术方式发觉计算机系统运行中出现的服务项目常见故障，从这当中评定安全隐患，制订维护计算机网络信息安全所使用的对策。如今在计算机网络运维中应用风险评定技术时，主要有两个需要明确和多多注意。一是计算机数据信息散播具有多种特点，风险评定技术必须监控和管理方法各传送连接点和信息构造，与此同时利用数据库中多种多样管理体系进行信息的发掘，充分了解存有的行为问题和信息。二是在运用风险评定技术时，要努力创造动态性、精准的剖析。这个时候就需要创建有关的数据库系统，全过程检测信息侵略途径，及早发现并妥善处理安全风险，避免对计算机系统运行安全造成影响<sup>[2]</sup>。

异构体结合技术的应用具备独特性，能够满足计算机互联网应用的诸多必须。从总体上，在互联网信息传输过程中，日志的数量和种类通常由一个或多个APP运用系统提供，导致系统自身的不同，务必及时纠正主要参数。因为达到最好实际效果，应注意提升单独系统运行管理体系，设定竖直和能力交叉式特点，将信息搭建放在一起，务求从整体上成功讲解计算机互联网信息。此外，使用异构体结合技术的过程当中，取决于检验技术，能够通过检测技术对处理数据信息评价，检验效率和效果都是毋庸置疑的。在做完早期数据分析处理

后,能够对业务执行竖直结合和总结。

管理决策技术在计算机网络运维中起着重要的作用是现阶段态势感知系统的关键所在技术能够对计算机网络运维的各个阶段进行检验。管理决策技术系统能够识别分辨计算机存放上存在安全隐患,也可以立即得知信息特性,精确对于某些信息进行监测、定位与解决。

### 3 影响计算机网络系统安全的因素

#### 3.1 人为主观操作

一般来说,互联网信息的传送和发布大部分由己实际操作,在具体传送中消极要素会严重影响信息自身。可是,考虑到用户本身缺乏安全意识的现况,在实际应用计算机时,没法严格执行实际操作要求开展解决,最后可能发生信息泄漏等诸多问题<sup>[3]</sup>。

#### 3.2 计算机硬件设备安全问题

计算机能够实现正常的相对稳定的通讯,与计算机里的硬件配置息息相关,针对现如今的计算机而言,不能正常的平稳安全运行在于硬件配置性能。为了能切实维护方便快捷的互联网连接水平,小型计算机、到到计算机应时而生,那应该得益于微处理器愈来愈小,计算机更方便携带。但是,依然存在诸多问题,网络黑客利用便捷性盗取和破译计算机信息,这给有关用户计算机形成了极大威胁。

#### 3.3 计算机软件安全漏洞问题

现阶段计算机软件在娱乐和操作过程中起着重要的作用,同时也给我们的生活带来很多便捷。在软件开发环节中,有关技术人员充分考虑了安全隐患,但还是有可能出现息息相关的技术系统漏洞,因而,很多计算机网络黑客和木马病毒利用网络漏洞侵略计算机,在其中文件现阶段,很多软件自身都具有修补作用,能够快速发觉计算机系统中系统漏洞并执行修补。利用该技术在有效阻拦病毒攻击的前提下,也可以切实维护计算机的安全和稳定性。

#### 3.4 黑客的故意攻击

计算机网络运行中容易受网络黑客攻击。现阶段,计算机网络具备开放性、公开性和共享性的特点,这也给黑客入侵带来了很大的机会。不法分子利用一台互联网设备,有可能会阻拦相关信息。比如,网络黑客根据获取用户的支付宝钱包(Alipay)账号和密码等个人隐私信息,可能会致使客户的经济损失。根据破译相关网址,也可以在后台管理获得相关的用户信息,经济发展伤害无法估量<sup>[4]</sup>。

#### 3.5 计算机网络技术的缺乏

在日常管理计算机网络的过程当中,务必解决大量

日志信息和报案信息,但是随着计算机网络的高速发展,愈来愈无法利用现阶段已知管理手段进行系统的统一管理。因此计算机网络管理人员也应加强相关的知识。现如今的计算机网络日益转变,每天都发生很多新的问题,若不能及时处理这种新的问题,不利于公司的发展。与此同时,要引导企业员工学习解决一般网络不稳定,在正常工作中,积极应对存在的问题,并呼吁大家一起来到网络安全管理方面。

### 4 计算机网络运维系统安全管理措施

#### 4.1 建立健全的信息管理制度

为了保证计算机网络运输系统的安全务必不断完善信息管理方案信息管理制度的内容主要包括以下几个方面。第一,认证客户真实身份。必须采用实名登记的办法验证客户个人身份,为运输系统的安全提供有力的确保。第二,建立完善的保密管理制度,增加客户信息维护幅度,尽量避免个人隐私泄露问题的发生。第三,确保安全管理规范化。工作员应严格按照相关规范,防止运维系统规范性实际操作、系统优化、系统漏洞问题的发生。第四,创建服务制度,逐步完善该体制,有效保障客户信息安全。第五,运用相关技术性对消费者进行科学授权。客户信息的可靠性、详细安全度。第六,严格把关系统中各种信息,及早发现和处置存有安全隐患,确保运输系统正常运转。

#### 4.2 提高网络安全保障

网络信息安全都是高效管理计算机网络运输系统安全的一种方法。你可以在计算机上安装防火墙和木马软件,根据按时扫描仪和检测等方式查验运输系统。这样不仅可以检验未知病毒,还能够合理监管运输系统的主页、文档、运行内存、电子邮件等,合理保障体系的安全运行。安装防火墙以前,请综合考虑计算机的总数。如果要必须维护一台计算机,则不需要软件网络防火墙。此外,假如计算机可以免费下载可以抵抗病毒进攻最新发布的补丁,则不需要安装防火墙。设置防火墙时,预防地区都是重点考虑内容。可在这个区域申请的信息数据信息务必合理布局,以统一安全防护运输系统。与软件网络防火墙对比,服务器防火墙防护效果更强,可自主运作,因而广泛用于计算机网络传输系统的安全管理<sup>[5]</sup>。

#### 4.3 硬件方面的维护工作

社会发展现代化发展不断深化,企业的发展离不开计算机参与其中。企业必须灵活运用计算机才可以紧跟社会的发展。计算机分成硬件与软件两个部分。计算机性价比高,企业整体工作效能好,与此同时能够实现企

业内网的高效运行。在挑选计算机硬件配置时应当注意不仅高度重视企业内部网络硬件设施的品质也需要高度重视企业外部网络硬件设施的品质付款后需要对相关硬件设施提升日常运送工作中,确保硬件设施正常启动。为了能硬件设施较好的软件环境,当环境因素恶劣造成硬件配置毁坏严重的话,也会增加硬件设施的维护费用,环境因素能通过人员的高度关注来预防。所以选择质量稳定的硬件设施同时加强硬件设施的日常维护保养工作就是企业日常相关工作的良好条件。

#### 4.4 最大程度提升终端入网的安全管理水平

以在计算机网络体系中优化提升交换机设备好几个连接接口的验证方式,针对性地设计方案辅助的互联网准入条件认证平台,最大限度地减少各种互联网故意侵略问题的发生几率。融合网络运维管理工作中的具体开展情况及各普遍安全隐患的重要原因、表达形式,对终端安全基准线模版开展优化提升,更新改造后终端设备接入方法具有很高的可行性分析,网络维护安全存在较大的局限储存和备份数据不一样终端产品用户各密匙信息,储存比如互联网IP地址等信息,即时对比终端产品用户的储存信息、端口号验证信息,高效地查验终端产品用户信息真实性<sup>[6]</sup>。

#### 4.5 优化计算机网络运营维护的各环节

要重视提升计算机网络运行管理的各个阶段,提升企业或事业单位的结构网络结构,有利于日常管理与企业决策工作中。根据对网络架构的改善,在一定程度上能够进一步提高计算机网络性能,满足客户的使用需求,并且在提升环节中关键完成专业性人才的应用。除此之外,还应当高度重视专业人员的计算机实际操作水准,针对目前相关工作人员安全意识淡薄的情况,提升相关人才团队的塑造,并定期举办相关活动,开展相关职业技能大赛活动,合理保证计算机操作流程规范和标准安全度在计算机网络运行安全维护保养的改善中,材料文档的梳理工作中不可忽视。材料文件信息梳理对确保计算机网络的安全运行具备很重要的作用,高度重视质量文件的归整工作中,选择适合自己的工作人员按时梳理相关材料文档,并且对相关员工进行,提升资料汇总工作效率。

#### 4.6 提高用户的计算机安全意识

计算机的安全离不开所有用户的协作维护保养。搞

好相关安全防范意识推广工作,根据相关微信公众平台和新闻媒体推广宣传相关专业知识的,推进群众应用上网安全,合理解决各种信息,提升企业工作效能,大幅度减少人力成本。

#### 4.7 改进数据加密技术

现阶段,根据对数据库加密系统的高效改善,赢得了互联网信息的安全和稳定性,在通过对应的完善化加工后,有效运用数据库加密系统,能够实现信息数据信息的全面确保,与此同时也可以实现用户授权的准确性,完成真实管理能力比如,在数据加密数据收集整理中,关键能够梳理两方面。对密文中并未数据加密处理原始记录请求;针对保密,主要是针对早已数据加密的信息,在相对应的解决操作过程中,主要考虑更换和置换等形式的的应用。其中,更换就是指规定原先的密文能直接转换成保密,更换通常是直接弄乱密文的最基本次序,并重新确立。在数据加密审核中,相关工作人员能将保密和密文相互结合,从而保证了数据信息的安全和稳定性,并且也保证了相对稳定的运维需求。

### 5 结束语

计算机网络运维和安全工作至关重要和必需,一定要予以特别重视,仔细做好计算机信息管理方法,加强风险管理幅度。对于计算机网络安全隐患,竭力注重计算机网络运维和管理的重要的地位,运用计算机信息技术性,避免比较常见的计算机网络安全隐患,与此同时断决计算机网络信息智能管理系统,实现更佳的计算机网络运维及安全管理。

#### 参考文献

- [1]吴亚辉,刘阳,张小超.计算机网络安全防御系统设计研究[J].中国新通信,2020(10):155.
- [2]刘秀彬.计算机网络可靠性优化设计研究[J].电脑编程技巧与维护,2020(03):148-149+171.
- [3]骆宏秀.计算机网络技术在电子信息工程中的应用[J].科技风,2020(35):106-107.
- [4]刘细苟,吴晔.计算机网络技术在电子信息工程中的实践探讨[J].信息与电脑(理论版),2020,32(19):23-25.
- [5]谢好.电子信息工程中计算机网络技术的应用分析[J].科技创新与应用,2021(6):179-181.
- [6]徐明磊.电子信息工程发展现状及保障措施[J].黑龙江科学,2019,10(10):136-137.