

医院网络安全与防范措施探析

王鹏祥

(东部战区总医院淮安医疗区,江苏淮安 223001)

摘要:在互联网技术快速发展下,对各行各业发展起到促进作用。尤其是对于医院来讲,通过“互联网+医疗”技术,有效提高医疗效率,患者也可以及时查看自己的检验检查报告等,通过互联网远程医疗,偏远地区和出行不便的患者在家就可以得到诊疗。但是在使用计算机网络时,还需要从保障网络安全出发,制定有效的防范措施,解决存在的网络安全问题,确保各项工作的顺利开展。

关键词:医院;网络安全;防范措施

中图分类号:R197

文献标识码:A

文章编号:1004-7344(2021)15-0268-02

0 前言

在医院运营与管理中网络安全技术已经成为比较重要的组成之一,一旦计算机网络出现安全问题,势必会影响各项数据与信息的存储与使用效果,甚至还会出现重要资源泄露等问题,影响医院的正常发展。因此在医院中就要从保障计算机网络安全入手,制定有效的防范措施,满足医院的运营与发展需求。

1 医院计算机安全的重要性

在科学技术不断发展下,计算机网络技术的运用范围明显增加,技术水平也在不断提升。尤其是在医院运营中,通过使用计算机网络技术,不仅可以提高医院运行效果,同时也可以保障医院运行的流程化发展,实现提升管理工作有效性目标,为医院稳定发展提供支持。在传统的管理模式中,所使用的管理方式存在着一定的局限性,影响精细化管理目标的实现,加之所使用的操作技术存在较强的复杂性,工作效果并不理想。但是在计算机网络技术的使用下,通过对不同系统进行整合,能够增强管理效果及运营管理效果。借助计算机网络技术能够为资源共享提供支持,展现医院信息与数据的价值,为各个部门工作科学化发展提供支持。因此在医院运营管理中就要从合理使用计算机网络技术出发,在保障计算机网络系统安全性的基础上提升对安全管理的重视度。只有确保计算机网络的安全,才能确保信息与数据等的安全性,满足后续工作需求。当计算机网络系统出现安全问题后,很容易出现信息丢失、泄露等问题,影响医院的正常运转。因此在现阶段发展中就要从做好计算机网络安全管理入手,运用信息技术与网络系统,在提升信息化建设程度的基础上提升管理能力,解决管理中的问题,满足各项工作开展要求^[1]。

2 医院计算机网络安全问题

2.1 病毒问题

影响计算机网络安全因素之一就是网络病毒,一旦计算机

系统被网络病毒入侵,很容易对所保存的数据与信息产生直接影响,甚至还会造成系统出现瘫痪等问题。当病毒入侵到医院中的计算机网络以后,很容易产生严重的损失,对医院正常运转产生不利影响,限制医疗卫生工作的开展。其次,容易出现医患个人信息泄露,对隐私信息的安全性产生不利影响,甚至还会上升到威胁人身安全等问题。对于网络病毒来讲,形成的主要原因就是编程人员在违背我国法律法规、社会道德等的基础上编写出具有恶意的程序,并植入计算机系统中,产生侵害问题。甚至不法分子还会利用病毒入侵医院中的计算机网络系统中,以远程控制等方式窃取、篡改数据与信息,产生信息泄露问题,威胁医院的正常运行等。

2.2 操作行为问题

医院在正常运行与管理中需要借助计算机记录患者的具体信息,从而全面掌握患者实际情况,发挥互联网共享性特点,针对患者病历信息进行细致的沟通。可以说借助计算机网络系统不仅可以降低工作人员工作压力,同时也可以避免因人为因素产生的记录失误等问题。但是也应当明确的是,计算机网络系统中涉及许多的计算机软件,而部分医护人员专业性不足,对计算机软件的认识并不全面,难以熟练操作计算机软件。在日常工作中很容易出现操作不当等问题,对计算机网络安全防范工作开展产生不利影响。其次,部分工作人员在使用习题中为了提高工作便捷性,存在没有设置、简单设置账户与密码现象,或是在同一习题中不同账户与密码完全一致,而这就降低计算机网络系统中信息资料的防护效果,存在安全隐患问题^[2]。

2.3 内部管理问题

医院在建设及使用计算机网络系统时,并未认识培养工作人员安全使用网络的意识与能力的重要性,也没有制定与之相适应的管理制度,使部分工作人员在日常工作中很容易出现操作

不规范等问题,如因个人操作不当进入非法网站中,而这也提高了病毒入侵的概率。其次,部分工作人员并未形成网络安全意识,也没有认识到保障数据信息安全的重要性,并未设置专门的账户与密码等。也正是受到多种因素的影响,使医院网络安全问题不断出现。

3 医院计算机网络安全防范措施

3.1 选择合理设备

在医院运营与发展中,所使用的计算机网络设备是否合理直接影响到计算机网络系统运行的稳定性。为了保障计算机网络设备的合理性,就需要从落实安全管理原则出发,确保管理工作的顺利开展。想要提高计算机网络设备选择的合理性,就需要从医院自身发展实际情况出发,坚持从不同层面进行分析,做好全面研究工作。①做好运行效率方面的考量。如从多模光纤出发,做好主线网络设置工作,在保障备份完整的基础上确保线路数据与信息的完整性,避免出现数据损坏、丢失等问题,对系统的正常工作产生不利影响;②做好医院中心机房设备配置工作。在这一环节中应当从保障规格合理、配置准确出发,满足网络系统整体运行需求。在中心机房中还应当配备专业管理人员,及时开展设备安全管理工作,定期针对设备进行维护保养,并配备备用电源等,避免出现网络安全事故;③确保中心机房环境的合理性,利用恒温恒湿环境,消除环境因素对机房设备的不利影响,保障设备的正常工作;④提升医院系统服务器配置标准,明确相关标准与要求,保障计算机系统网络运行的安全性与稳定性。由于服务器不同,所以在管理中需要确保服务器之间的稳定运行,在保障备用电源充足性的基础上确保计算机网络系统的不间断运行^[4]。

3.2 选择安全系数高的杀毒软件

在医院中要求管理部门应当及时做好计算机网络系统安全管理工作,从实际情况出发,选择安全系数高的杀毒软件,利用防火墙等提升医院计算机网络系统安全防护能力,避免出现病毒入侵等问题。设置防火墙的目的就是要确保信息传输过程的安全性,提供适合的传输渠道,在快速识别病毒的基础上避免出现安全事故。同时还需要确保其安全性与便捷性,针对医院计算机网络系统防护实际情况进行分析,定期开展病毒查杀等工作,在保证防护工作及时开展的基础上确保系统的安全性。

3.3 提升管理技术与能力

首先,在医院中要求各个部门中应当及时掌握计算机网络系统、服务器管理方法,尤其是对于服务器相对较多的医院来讲,应当借助其他服务器实现对计算机网络系统的安全有效管理,提高检测效果,保障信息数据接收与传递的合理性,即便常用服务器出现问题,也可以保障系统的正常工作。其次,打造良好的计算机网络环境。在医院中应当及时针对计算机设备开展维护与检查工作,找出计算机设备在适应中可能出现的问题,在及时更新软件的基础上做好防潮、防火等处理,确保计算机网络运行环境的质量。最后,提升对数据与信息保护管理的重视度。通过使用实时监控设备端口,以此掌握计算机的实际情况,实现提前

预防病毒入侵目标^[4]。

3.4 开展专业化培训活动

首先,在医院中应当及时组织工作人员参与专业化的技术培训,在完善培训制度的基础上确保计算机网络安全管理工作的顺利开展。通过将计算机网络安全管理内容纳入培训计划中去,确保工作人员能够掌握最为先进的管理方法与技巧。其次,应当组织专业人员针对工作人员在日常工作中遇到的问题进行处理,帮助工作人员解决存在的问题,不断提升工作人员在操作环节中的规范性,提升问题解决问题,保障计算机网络安全,提升网络安全管理能力。最后,开展计算机网络维护培训工作。在工作中应当从实际操作环节出发,针对存在的安全问题进行分析,采取有效的维护处理措施,实现对网络隐患的有效控制。

3.5 完善安全管理制度

医院想要确保计算机网络安全灌流工作的顺利开展,就需要建立专属的计算机网络安全管理制度,以此提升整体安全维护管理能力,在及时消除安全隐患的基础上保障管理工作顺利开展。医院中的工作人员也要坚持从完善管理制度出发,明确岗位安全管理责任,真正将责任落实到具体中,在提升工作人员责任意识的基础上主动将所掌握的操作方法运用到工作中去。通过组织安全管理人员参与培训,在提升管理与服务能力的基础上展现计算机网络系统作用。其次,需要做好数据备份工作。为保障网络系统的正常工作,就需要从提升数据安全性出发,在及时开展数据备份的基础上避免因网络攻击等问题出现数据丢失、损坏等问题。通过对数据信息类型进行分析,以此来采取适合的备份方式,在掌握具体情况的基础上制定有效的培训计划,保障数据备份的完整性。

4 结语

综上所述,在新时期发展下,就需要从做好医院计算机网络安全管理工作入手,针对存在的安全隐患进行分析,制定出有效的安全对策与防范措施,在防御攻击的基础上确保数据与信息的安全性,为医院内部稳定发展提供支持。

参考文献

- [1] 刘超.医院计算机网络安全隐患及防护措施探析[J].电脑迷,2017(4):37-38.
- [2] 李静旭.医院计算机网络常见安全问题及防范措施[J].中国保健,2010(11):122.
- [3] 严红岭.医院计算机网络安全隐患的分析与应对[J].各界,2020(8):189.
- [4] 徐瑾.医院计算机网络安全与防范措施[J].医学信息(西安上半月),2006(8):28.

收稿日期:2021-03-07

作者简介:王鹏祥(1990—),男,汉族,江苏沐阳人,本科,工程师,研究方向为网络安全、数据中心建设、医院信息化建设。