

关于医院计算机网络安全管理工作的维护策略分析

胡杨

(邯郸市中医院, 河北 邯郸 056001)

【摘要】随着我国科学技术的不断发展, 计算机网络技术在各行各业中得到了广泛的应用, 也给人们的生活带来了极大的便利, 特别是计算机网络技术在医疗领域中的应用有效地提高了医疗行业的工作效率, 但是在计算机网络技术使用过程中存在着很多问题, 加强计算机网络安全管理工作也变得尤为重要。本文基于医院计算机网络安全管理的意义, 就当前我国医院计算机网络安全管理工作存在的问题进行分析, 并提出了加强医院计算机网络安全管理工作的有效策略。

【关键词】医院; 计算机网络; 安全管理; 维护策略

引言:

医院的信息系统主要包括管理系统、医疗系统、业务系统、电子病历系统等, 这些信息系统都是以计算机为基础, 通过网络技术来实现信息共享。计算机网络安全管理是医院管理的重要内容, 不仅涉及医院的信息安全和利益问题, 还关系到患者的医疗安全。因此, 提高计算机网络安全管理水平, 确保计算机网络的安全性和可靠性, 是保障医院工作正常开展的重要内容之一。

一、医院计算机网络安全管理的意义

随着互联网时代的到来, 医院计算机网络管理工作也面临着全新的挑战和机遇, 如何充分发挥计算机网络在医院医疗活动中的作用是医院管理人员必须深入思考和探讨的问题。通过提高医院计算机网络安全管理水平, 能够保证医院信息系统运行安全稳定, 减少医院信息系统出现故障导致患者就医困难的现象发生。

(一) 充分发挥医院的资源优势

医院计算机网络的建设是一项系统工程, 需要各部门的共同参与和合作, 在建设过程中充分发挥各部门的资源优势。在设计网络建设时将医院信息管理系统、HIS系统、临床工作流程管理系统等结合起来形成一个完整的网络, 整合信息资源, 为医院其他工作的开展提供便利条件, 例如医生可以利用电子病历来进行诊治和医嘱, 利用电子病历对病人进行追踪。

(二) 为医院提供更加优质的服务

医院作为为人们提供医疗服务的单位, 在进行计算机网络安全管理时, 应始终将医院的整体利益放在第一位。由于计算机网络技术的不断发展, 医院要想在竞争激烈的市场中获得一席之地必须重视

自身服务水平, 计算机网络技术可以对医院进行全面了解, 也可以及时向患者提供相关信息, 患者可以通过计算机网络技术了解到自己的身体状况以及是否需要到医院进行进一步治疗, 因此, 将计算机网络安全管理放在重要位置可以使医院提供更优质的服务。

(三) 有利于医院信息化建设

医院信息系统是医院重要的信息资源, 是医院信息化建设的重要组成部分。医疗业务管理系统、药品采购管理系统、人力资源管理系统等都离不开计算机网络。因此保证计算机网络安全, 防止病毒和黑客攻击, 对加强医院信息化建设具有重要意义。

(四) 为医院提供准确的数据资料

医院在运行过程中会产生大量的数据资料, 这些数据资料如果不能及时整理很容易出现误差, 影响医院的正常运行。由于计算机网络是一种动态的信息交换系统, 数据是实时更新的, 通过对这些信息进行加工整理可以及时地将各种信息进行反馈、传输、保存。医院通过计算机网络系统可以将来自各个部门的各种数据资料进行集中处理, 使这些数据资料在医院内部形成一个统一的数据库系统, 从而提高数据资料的准确性。

二、医院计算机网络安全管理工作存在的问题

随着医疗水平的不断提升, 医院也越来越注重信息化建设, 采用计算机网络技术是现代化发展的必然趋势。目前医院计算机网络安全管理工作还存在很多问题, 医院必须对此引起重视, 采取有效的应对措施解决计算机网络安全管理工作中存在的问题。

(一) 医院计算机系统软件的漏洞

医院的计算机网络系统是一个开放性的系统, 随

着医院业务的不断增加,对计算机网络系统的需求也随之增加,使得很多软件厂商为了赚取更多的利润而加大对软件的开发力度,但是由于开发人员专业水平和技术水平有限,软件系统的漏洞也随之增多,比如一些医院的信息管理软件在设计时可能并没有考虑到用户操作习惯和一些特殊情况,而一旦有用户使用不当就会导致信息泄露和丢失,给医院造成损失。

(二) 医院信息安全管理制度的不完善

医院信息系统在运行的过程中受到多种因素影响会出现不同的故障,在对这些故障进行排除时需要专业人员的配合,但是,实际工作中很多工作人员并没有掌握信息安全管理制度的内容,对故障问题也不能及时发现并解决,这些问题都会增加计算机网络安全管理工作难度。同时,在医院信息系统运行的过程中需要对重要数据进行备份,但是很多医院并没有配备完善的备份设备和技术人员,出现问题后并不能及时修复和处理,这就增加了医院信息网络安全管理工作的难度。

(三) 医院计算机系统维护人员素质参差不齐

随着医院信息系统的不断升级,工作人员要不断地进行学习与更新才能适应系统的发展,需要计算机系统维护人员具备一定的专业技术。但是,部分医院中从事计算机系统维护工作的人员并不是计算机专业毕业,其所接受的教育与培训也比较有限,这些人只是普通的计算机操作人员,并不具备较高的专业知识水平与技能,使计算机系统维护工作存在一定的困难。如果计算机系统出现了问题,其维护人员也不能及时有效地进行解决,使得医院在计算机系统运行过程中存在较大的风险。

(四) 网络安全意识薄弱,缺乏有效的安全防范措施

医院网络安全问题主要体现在内部管理和外部攻击两方面,内部人员缺乏网络安全意识,网络安全防范措施不完善,缺乏对计算机的日常维护和管理,导致信息的泄露、丢失,甚至出现病毒入侵。外部攻击方面主要是指黑客、病毒入侵等,由于网络的开放性,黑客可以通过技术手段获得大量的信息资源,对计算机进行攻击、破坏等。随着计算机网络技术的发展,网络犯罪现象日益严重,医院作为社会公众服务行业更是成为犯罪分子攻击的重点对象,因此加强医院网络安全意识,增强网络安全防范措施非常重要。

三、医院计算机网络安全管理工作的维护策略

(一) 完善医院信息安全管理制度的完善

医院在进行网络安全管理的过程中要做到责任

到人,不仅要落实到每个部门和岗位上,还要落实到具体的责任人身上。医院要制定出详细的网络安全管理制度,内容包括设备维护管理制度、设备升级与更新管理制度、网络系统维护管理制度等,在出现问题时要明确划分责任。对此,医院需要建立健全计算机网络安全管理的规章制度,明确计算机网络安全管理的具体要求和措施,做好网络安全建设工作和医院内部信息系统的建设工作,确保计算机网络安全建设与信息系统的安全运行。

(二) 及时更新系统的补丁程序

医院的计算机网络系统由于其规模较大,使用范围广,所涉及的服务器较多,所以在很大程度上给系统的安全性带来了威胁。

一旦计算机网络系统被恶意攻击就会导致整个医院网络出现瘫痪,不仅给医院带来经济损失,也会影响医院工作人员的工作。因此在计算机网络系统运行过程中要注意对系统进行及时更新,通过补丁程序来对计算机系统进行修补。目前在国内应用较多的补丁程序主要是Windows操作系统下的Windows system install windows update等。而在医院中应用的计算机网络系统大多是Windows操作系统,其安装后要进行自动升级。在升级的过程中要注意将操作系统的漏洞一并修复,避免出现安全隐患。通过补丁程序来对计算机系统进行升级可以避免出现严重的安全问题,从而提高计算机网络系统的安全性。当前医院使用比较多的补丁程序有Microsoft公司提供的Windows Update等,这些补丁程序在医院中使用较为广泛。

(三) 做好网络病毒的防护

首先,要做好计算机病毒的检测工作,在病毒被发现之前就对其进行阻止可以大大提高计算机网络的安全性。医院应该建立一套完善的计算机网络安全检测系统对计算机系统进行定期检查,保证计算机网络运行的安全性。在对系统进行检查的过程中要注重对用户身份的审核,避免出现用户身份被冒用的情况发生。其次,要做好系统漏洞的修复工作,医院应该及时更新计算机系统中存在的漏洞和缺陷,建立完善的安全补丁机制,保证医院计算机网络系统在运行过程中不会出现漏洞。此外,还可以建立一套完善的安全预警机制,当用户出现异常操作时及时报警和提醒。最后,要做好计算机病毒防护工作,在使用计算机系统过程中对计算机系统进行定期备份和维护工作,防止病毒通过U盘等传播方式在医院内传播。一旦发现病毒入侵系统或计算

机硬件设备后及时进行处理,对重要文件进行备份和加密处理。

(四) 做好网络数据传输中的保密工作

做好网络数据传输中的保密工作主要是从网络数据传输的保密性方面入手对医疗信息进行保护。首先,要保证医院内部数据传输的保密性,需要相关人员在网络信息传输过程中做好保密工作,在进行数据传输的过程中采用加密技术对传输的信息进行加密,确保医院内部的数据信息不会被其他用户窃取。其次,保证医疗数据传输过程中的保密性。在医疗数据进行传输之前对这些数据进行严格的检查和鉴定,保证数据的准确性和安全性,医院内部管理人员需要对医疗数据信息进行详细记录,交由相关人员对其进行进一步的处理。最后,在进行医疗信息传输时需要有专门的工作人员对其进行监管和操作,确保医疗信息能够按照医院内部的要求来完成,避免其他人恶意篡改或者删除医疗信息。

(五) 加强计算机硬件与软件的安全管理

对于计算机的硬件和软件安全问题,医院工作人员在日常工作中需要做好全面管理工作,保证计算机硬件与软件能够得到良好的运行状态,计算机硬件与软件的安全管理包括以下几个方面:1. 硬件管理方面。医院工作人员要严格检查计算机各部件是否能够正常运行,如果发现问题要及时处理;2. 软件管理方面。医院工作人员在日常工作中需要对医院计算机网络系统进行定期检查,检查内容包括操作系统是否稳定、杀毒软件是否有效、补丁程序是否完整等等,医院工作人员需要对网络系统进行定期更新,保证网络系统能够具有较高的安全性,建立完善的防火墙机制,保护医院计算机网络系统不受到外来网络攻击,有效防止外部恶意攻击对医院计算机系统产生不良影响。

(六) 加强医院网络安全管理人员的培训

在医院网络安全管理工作中需要对相关工作人员进行网络安全教育,提升工作人员的计算机网络安全意识。医院应该定期组织计算机网络安全教育,通过培训的方式提升工作人员的安全意识,加强个人素质修养,提升工作人员的专业水平和职业素养。同时,医院应通过制定网络安全管理制度来约束工作人员的行为,将相关法律法规作为重要内容,在对医院计算机网络安全管理人员进行培训的过程中进行定期考核和监督。考核主要包括三个方面:考核工作人员对于相关法律法规的掌握程度;考核工作人员对于医院计算

机网络管理制度的执行程度;考核工作人员对相关技术知识的掌握程度。通过对以上内容进行考核和监督促进医院计算机网络安全管理工作的顺利开展。

(七) 信息加密技术的应用

信息加密技术的应用能够在很大程度上减少网络信息被盗取的可能性,有效提高医院计算机网络安全管理的有效性。使用加密技术能够对计算机网络数据信息进行加密,并在计算机网络运行中将加密技术的优势充分发挥出来。由于医院受到网络安全管理机制不完善以及网络技术人员自身操作不规范等因素的影响,会导致医院计算机网络信息数据被窃取和篡改,数据信息加密技术的应用能够提高数据信息的保密性以及安全性。

(八) 数据网络备份

医院数据网络备份主要包括数据存储备份和数据恢复备份,其中数据存储备份是指将医院重要的数据资料进行物理形式的保存,当发生不可预测的安全事故时可以及时地恢复相关信息。而数据恢复备份则是在网络正常运行时利用软件、硬件等对网络中出现的安全故障进行处理,将出现故障的网络系统进行自动恢复。在对医院计算机网络系统进行维护时要注意将网络安全问题的防范工作作为重要内容,将其列入日常工作中。

四、结语

医院计算机网络的信息安全管理是一项长期的工作,管理人员在关注信息安全的开发和运用的同时也应该积极地探索和学习新的信息保护技术,提升信息安全的管理水平,从而为医院网络安全管理工作提供可靠的保证。

参考文献:

- [1]谷红雨.企业计算机维护现状及解决对策要素探索[J].中国宽带,2022,18(9):182-184.
- [2]杨雷.医院计算机网络的安全管理措施分析[J].集成电路应用,2023,40(7):277-279.
- [3]柯传琪.医院信息处网络安全建设研究[J].科技风,2023(26):65-67.
- [4]刘吉祥.医院计算机网络信息系统的安全风险与控制策略[J].科学技术创新,2018(32):94-95.
- [5]刘舰.浅析计算机信息系统维护与网络安全漏洞处理策略[J].网络安全技术与应用,2019(4):2-4.
- [6]东述樾,赵娜.关于医院计算机网络安全管理工作的维护策略分析[J].世界最新医学信息文摘,2018,18(74):198-199.