

医院信息系统安全风险管理的有关研究

Research on Security Risk Management of Hospital Information Systems

付子峰 冉静 通讯作者

Fu Zifeng, Ran Jing, Corresponding Author

(重庆大学附属三峡医院 重庆 404000)

(Chongqing University Affiliated Three Gorges Hospital Chongqing 404000)

摘要: 随着信息化时代不断发展, 信息系统被应用到医院的日常管理过程中, 发挥着至关重要的作用。但是在信息被录入、处理和存储的过程中还是存在着安全方面的风险, 现阶段对于医院中的信息系统提出了更高层次的要求, 解决现存的安全风险, 实现医院信息系统的升级和完善。本文将阐述安全风险管理的概念, 针对医院信息系统安全管理的现状进行综合分析, 证实安全风险管理的必要性, 并对于现阶段医院信息系统安全风险上存在的不足进行研究分析, 提出相关的有效措施来解决不足, 达到医院信息数据安全的效果。

Abstract: With the continuous development of the information age, information systems have been applied to the daily management process of hospitals, playing a crucial role. However, there are still security risks in the process of information input, processing, and storage. At present, higher level requirements have been put forward for information systems in hospitals to address existing security risks and achieve the upgrading and improvement of hospital information systems. This article will elaborate on the concept of security risk management, conduct a comprehensive analysis of the current situation of hospital information system security management, confirm the importance of security risk management, and conduct research and analysis on the shortcomings in current hospital information system security risk management. Relevant effective measures will be proposed to solve the shortcomings and achieve the effect of hospital information data security.

关键词: 医院; 信息系统; 安全风险

Keywords: Hospital; Information system; Security Risk Management

随着我国计算机技术不断完善, 将网络和生活高度的融合在一起, 网络成为人们生活的重要组成部分, 利用计算机技术帮助医院进行信息方面的管理, 实现医院的信息化管理。医院的信息系统很大程度上帮助医生整合处理患者的信息数据, 但是同样医院信息系统也面临着巨大的安全风险的问题, 要在医院信息系统使用过程中添加安全风险管理方面的内容, 依照医院对于信息数据的真正需求, 规定出相应的安全风险管理制度, 针对患者的信息数据进行严格的保护和处理, 真正实现有效的信息数据管理, 发挥出安全风险管理制度最大作用, 渗透到医院信息系统的每一个环节中, 保障医院信息系统的正常运转, 保证医院的稳定发展。

一、安全风险管理的理念

医院信息系统的安全风险管理是保障医院所有业务正常运转的关键, 医院信息系统覆盖于医院的全部业务, 应用到医院的多个领域, 比如科研方面、临床医学以及医院内部管理等, 帮助医院利用科学全面的方式来处理信息数据, 达到信息自动化的程度。现阶段在使用信息系统的安全风险管理过程中, 主要分成两个控制手段, 一是信息方面的识别, 二是信息方面的控制^[1]。在应用信息系统的过程中, 利用信息方面的识别来对于医院内部的信息数据进行全天无休的监管, 以此来防止安全风险的产生。一旦医院的信息系统发生风险, 信息系统的安全风险管理快速对其进行信息方面的控制, 以此来化解信息系统的风险, 将医院的损失降到最低, 加强医院的防御能力, 信息系统定期升级优化。

二、医院信息系统安全管理方面的现状

(一) 可以被攻击的渠道太多

目前的计算机技术越发先进, 信息系统将整个医院覆盖住, 被应用到医院的各个流程中, 应用的越发广泛, 从线上的预约挂号开始, 整个治疗过程都被信息系统覆盖, 例如线上缴费、手机预约以及远程查看治疗情况等, 每一个环节都充斥着信息系统的应用, 这样的状况意味着多媒体终端开始成为信息系统的重要组成部分, 为医生和患者带来巨大的便利的同时, 也同样带来了安全方面的风险。在信息系统和计算机技术连接越多的时候, 信息安全问题成为首要需要解决的问题之一, 可以被攻击的渠道开始变多, 信息的安

全问题至关重要。在医院信息系统被应用的过程中, 带来便利的同时, 也会同样程度上增加安全方面的风险, 导致出现系统上的漏洞^[2]。

(二) 被攻击的范围在不断扩大

随着信息化时代的到来, 不仅仅是计算机技术被广泛应用到现实生活中, 黑客拥有的计算机技术也在不断的更新完善, 掌握攻击医院信息系统的能力, 黑客的“病毒”也在变强, 因此现阶段的黑客攻击的范围在不断扩大, 具备着破坏力强、攻击范围广以及散发速度快等特点, 黑客使用不正当的手段在医院的信息系统中种植病毒, 病毒在医院的信息系统中快速繁殖, 生存在每一个角落中。以此来攻击信息系统, 导致信息系统的安全受到威胁, 甚至信息系统有可能瘫痪, 黑客通过这样的手段获取到医院的全部信息^[3]。

(三) 传播的速度十分迅速

黑客的技术逐渐高深, 黑客手中的病毒破坏力和偷取信息的能力也在不断增强, 在黑客利用病毒攻击医院的信息系统过程中, 病毒强势的入侵医院的信息系统, 强占信息的传播途径, 通过该传播途径快速传输病毒到信息系统的信息库, 开始发送一些无用的信息, 阻拦医生操作计算机, 在极短的时间内完成信息系统崩溃的效果, 严重影响到医院的正常运作, 医院的工作流程被打破。不仅仅是影响到医生和患者的治疗过程, 还导致信息系统中的信息面临着泄露的风险, 为医院带来了相当严重的损失, 造成医疗事故的发生。

三、医院信息系统安全风险管理的必要性

医院信息系统的安全风险管理十分的重要, 针对现阶段医院信息系统安全风险管理存在的问题, 例如对于信息系统的安全问题不够重视、信息系统所需的安全技术方面存在不足、没有将信息系统的安全风险管理进行有效落实以及信息系统安全风险管理监管制度不够完善等, 针对现阶段医院不具备完善的医院信息系统安全风险管理制度, 为医院带来不同程度的伤害, 影响到医院信息系统安全风险管理发挥价值和作用, 导致医院发生信息泄露的情况。医院信息系统安全风险管理可以将其出现的问题进行及时的解决, 从源头上保障信息系统的安全问题, 避免问题带来的重大损失, 防止医院信息系统的无效工作, 减少在信息系统运行过程中产生的风险和

安全隐患^[4]。

四、医院信息系统安全风险管理的有效措施

(一) 信息系统中添加双核心网络的管理

医院要想利用好信息系统,发挥出信息系统的作用,首先需要做好医院信息系统的安全风险管理,维护好信息方面的安全,保障网络传输的效率。于是,在医院的的信息系统中添加双核心网络的管理,双核心网络是将信息系统的核心分在两台高端交换机来进行信息处理,利用两台高端交换机轮流使用,分担出信息系统的工作重心,同时将两台高端交换机利用信息技术虚拟成一台高端交换机,使用光纤将两台高端交换机进行连接,实现两台高端交换机的信息共享和信息传输。网络之间利用千兆光纤连接,保证信息传输的速度迅速,再使用 IRF 技术实现双核心网络。添加成功之后,两台高端交换机轮流进行工作,一旦高端交换机出现故障,另一台高端交换机还是可以承担起信息方面的工作,不至于全面崩溃,双核心网络为医院信息系统正常运行提供最为坚实的保障,同时也为维修争取了时间,保障医院信息系统稳定运作^[5]。

(二) 对于医院信息系统管理平台进行定期的维护和升级

在医院使用信息系统的过程中,根本无法完全避免信息系统出现故障和受到攻击,但是可以增加信息系统的防御能力,来对抗病毒的侵入。于是对于信息系统要进行定期的维护和升级,有效的降低病毒侵入方面的风险。在信息系统运作过程中,要针对高风险的病毒进行专门的研究和记录,并将研究分析出的结果输入到信息系统的安全风险数据库中,对于数据库记录的病毒,信息系统可以快速发现并将其解决,有效的防御病毒的攻击,避免因病毒侵入导致的信息泄露^[6]。为了增加医院信息系统的安全方面的系数,要在信息系统中添加专门的保护机制,利用保护机制来保障信息系统中的信息安全,确保患者的个人信息不被侵害,针对不同的人员开放不同的访问权限,给予信息最大程度的保护。对于信息系统中的信息库进行分级管理和分层管理,给予不同等级的医生不同的信息权限,在访问权限设置方面,来设置出不同多样的等级制度,使得信息库里的信息被灵活的应用,信息系统为不同的等级赋予不同的权限,实现信息系统的科学全面的管理。为了保障医院信息系统安全风险管理的有效和高质量,对于医院信息系统管理平台进行定期的维护和升级,因此来满足医院对于信息系统的功能需求,将最为有效新型的计算机技术应用到信息系统中,全方位的提高信息系统的服务效率,及时处理医院信息系统管理平台出现的漏洞,将医院信息系统管理平台进行升级,不断完善医院信息系统管理平台中的功能,最大程度上提高医院信息系统安全风险管理的的能力,保证安全风险管理的的有效性,将病毒隔离在信息系统之外。

(三) 完善医院信息系统安全风险管理制度

医院想要提高信息系统的安全风险预估能力,必须要完善医院信息系统安全风险管理制度,需要为信息系统找寻一个行为准则。例如,做好完善医院信息系统安全风险管理的监管制度,最大程度上发挥出医院信息系统安全风险管理制度作用,在医院的内部管理中建立起信息系统安全风险监管小组,将安全风险的意识输入到医院的每一位医生的大脑中,成为需要遵守的原则中的一部分,利用信息系统安全风险监管小组来把控信息系统安全风险,信息系统安全风险监管小组的主要工作内容是对于信息系统安全风险管理的规范化和合理化,定期发展信息系统安全风险管理的研讨会,针对近阶段信息系统安全风险问题进行研究分析,及时将问题解决,增加整个医院关于信息系统安全风险方面的交流沟通。严格遵守信息系统安全风险管理制度,对于违背管理制度的医生进行严

肃处理,将信息系统出现的问题进行总结分析,不断完善信息系统的管理制度,提升信息系统的安全性和稳定性^[7]。

(四) 对于医院信息系统安全负责人员进行技术方面的培训

随着信息系统逐渐在医院中占比增加,需要医院中的医生掌握信息技术相关的专业知识,于是,对于医院的工作人员进行培训学习,以此来提高工作人员的信息应用能力,提升信息技术有关的专业素养,保障医院的工作人员可以顺利的完成信息系统的使用,在操作信息系统的过程中,减少操作失误的可能性,从侧面降低信息系统出现故障的情况发生。在培训医疗工作人员的过程中,需要采用科学有效的教学模式来进行信息技术专业知识的教学,建立起信息技术教学体系,帮助医疗工作人员提升信息技术的水平,逐渐完成医院自动化的想法,实现医院转型的服务状况^[8]。与此同时,在医院信息系统维护方面,也是需要维护人员具备专业的信息技术相关知识,针对医院信息系统安全风险管理人员进行专门的培训,最大限度的做好信息系统的维护工作。随着黑客的技术不断提高,想要抵抗住黑客的攻击,医院需要具备可以应对的信息技术,如果医院没有重视信息技术的培训学习,不提高医院配备的信息技术,医院在信息系统安全风险方面处于不合格的状况,时刻面对着信息系统安全方面出现问题的情况,一旦黑客入侵了医院的信息系统,信息系统中的信息将不再安全,时刻面临着信息泄露的局面,还无法做出及时的处理回应。因此,医院信息系统安全负责人员进行技术方面的培训是一件极其重要的事件,必须被执行,及时刷新医疗人员的信息技术,学习最先进的信息技术。在医院招聘的过程中,提高信息管理方面的门槛,需要掌握一定程度的信息技术,尤其是医院信息系统安全风险技术,并且在入职之前将医院信息系统安全风险制度掌握。

(五) 对于医院信息系统的安全风险管理进行严格把控

信息系统逐渐成为医院必备的工作环节之一,发展趋势十分猛烈,要在医院中实现信息系统的规模化,首先需要将信息系统中的信息进行考量分类,保证信息系统的高效,信息系统的安全风险管理主要包括监测、抵抗以及恢复这三个方面,每一个方面都发挥着自身的价值,具备着截然不同的功能,拥有着至关重要的地位。在信息系统的运作过程中,每一方面出现问题,都会严重影响到信息系统的最终作用,导致信息系统出现安全方面的风险,引发一系列的麻烦。因此,在信息系统使用的过程中,需要严格把控医院信息系统的安全风险管理的每一个细节,保障每一个方面都可以正常的运行,同时定期定时的进行相应的升级优化,尤其是信息系统的抵御功能,在信息系统中安装网络抵御系统,避免医院信息系统被恶意攻击^[9]。

结束语:

综上所述,随着计算机技术不断发展,很多行业开始依赖于计算机技术,现阶段的医院在经营过程中十分依赖于信息系统,以此要保障信息系统的安全问题,降低风险出现的几率,帮助医院更好的治疗患者。

参考文献:

- [1]张舒.网络环境下医院信息系统数据安全保障体系构建研究[J].网络安全技术与应用,2023,266(02):60-61.
- [2]吴庆斌,黄之怡.真实世界复杂交互环境下医院信息系统效能影响研究[J].中国信息化,2022,343(11):37-41.
- [3]卢生玉.基于虚拟化的数字孪生医院信息系统建设[J].山西电子技术,2022,225(06):53-55.