第 1 卷◆第 1 期◆版本 1.0◆2023 年
文章类型：论文|刊号（ISSN）：2972-4007(P) / 2972-4015(O)

探析医院信息系统的网络安全维护

吴悠悠
DOI:10.12238/deitar.v1i1.5896

[摘　要] 信息系统的安全运行对于现代医院的正常运营具有重要价值,其能够对医院运营过程中产生的数据资料进行科学管理,有效提升了医生护士的工作效率和医院的数据资料管理效率。信息系统在医院的应用过程中,有助于相关资料查询、就诊病患的诊疗活动开展、不同科室资料的共享(比如门诊资料、财务科资料等)等,强化了相关科室、部门与单位之间的密切联系,同时减少了医院运营管理成本。然而其在具体运行时,由于会受到人员设备因素、系统风险以及外来病毒攻击等影响,使得医院信息系统网络存在不同安全风险,比如就诊资料遗失、科研档案资料不完整、重要机密资料被外泄等,从而威胁到患者就诊、医学科研项目等开展,有些机密资料甚至还会威胁到国家安全。因此为了保障医院信息系统的可靠运行与相关数据资料安全,必须结合其实际运行状况,采取有效措施,加强对其进行安全方面的维护,从而规避数据遗失、确保科研档案资料完整以及防止信息系统崩溃等。
[关键词] 医院信息系统；网络；安全维护；安全风险
中图分类号：TU246.1　文献标识码：A

Analysis of Network Security Maintenance of Hospital Information System

Youyou Wu

[Abstract] The secure operation of information systems is of great value for the normal operation of modern hospitals. It can scientifically manage the data generated during the hospital operation process, effectively improving the work efficiency of doctors and nurses and the efficiency of hospital data management. In the application process of information systems in hospitals, it helps to query relevant information, carry out diagnosis and treatment activities for patients, and share information from different departments (such as outpatient data, financial department data, etc.), strengthening close connections between relevant departments, departments, and units, while reducing hospital operation and management costs. However, during its specific operation, due to the impact of personnel and equipment factors, system risks, and external virus attacks, the hospital information system network has different security risks, such as the loss of consultation information, incomplete scientific research archives, and the leakage of important confidential information, which threatens patient visits, medical research projects, and even national security. Therefore, in order to ensure the reliable operation of the hospital information system and the security of relevant data, effective measures must be taken to strengthen the maintenance of its security in combination with its actual operation, so as to avoid data loss, ensure the integrity of scientific research archives and prevent the collapse of the information system.
[Key words] hospital information system; network; safety maintenance; safety risks

医院信息系统主要是由计算机硬件系统、软件系统与网络系统等构成,其可靠运行,能够对医院数据资料(主要包括医生护士、就诊病患以及医学科研等信息档案)开展科学管理,使医院的数据资源得到共享,并且加强了不同科室、不同部门和单位之间的联系,从而为医院在开展医疗诊治活动与医学研究等方面提供数据参考。但是医院信息系统在实际运用过程中,由于受到诸多因素的影响(比如制度、作业人员、设备、病毒以及网络等),有可能造成医院产生的数据资料信息丢失、不完整等现象,使其存在很多安全问题,同时给不法人员留下了窃取相关数据的安全漏洞,严重影响了医院数据安全及其社会经济效益,还制约了医疗诊治工作的有效实施,并且威胁到医学科研工作的进展。因此为了确保医院信息系统网络的安全运行,本文概述了医院信息系统与网络安全,对医院信息系统网络安全现状问题开展了讨论分析,并结合实际,提出了医院信息系统的网络安全维护措施

1 医院信息系统与网络安全的概述

文章类型：论文|刊号（ISSN）：2972-4007(P) / 2972-4015(O)

1.1医院信息系统的概述。(1)涵义。信息系统建设是促进现代医院建设管理发展的主要举措,其有利于提升医院的相关管理工作效率和促进医院发展。医院信息系统作为数字化管理系统,其主要是运用先进的现代化技术(网络技术、通信技术、大数据技术、计算机技术等),对医院经营活动产生的数据资料实施收集、整理、分析与应用等开展管理(包括医生护士的人事管理、药品采购及其管理、病患就诊的医疗管理、医学科研资料以及医院基建等),简而言之就是对医院经营过程中的人、物、财等相关信息资料进行管理,从而提升医院管理工作开展的效率与效益。(2)特征。医院信息系统在实际运行时,其特征显著,具体表现为：第一,模块特征。医院的信息系统是由不同模块组成(比如病患就诊模块、药品采购模块、医学科研模块等),其在不同适用范围都能够发挥其作用。并且医院运行需要很多医生护士、相关科室与部门、以及相关单位的执行和支持,其运营范围主要为病患就诊与医学科研,也包括药品采购储存以及发放、医疗器械采买与操作保养、医院基建工程建设等,开展这些活动会产生大量的数据信息,而信息系统在不同项目活动中的应用,其相关模块的应用,都能够有效提升医院的管理效率与质量;第二,整合优势特征。由于医院在经营过程中,涉及的管理内容比较多(不同科室部门管理、药品器械采买储存管理等),并且不同内容其应用信息系统模块区别也很大,其管理要点也存在很大差异,所以为了提升管理效率与质量,必须加强对其信息系统各模块的整合。通过做好不同模块之间的整合工作,使信息系统在医院运营中的功能价值得到合理展现；第三,共享优势特征。医院信息系统包括医院经营活动中产生的绝大部分信息资料,并且不同科室、不同部门等都是密切相关。因此需要借助先进的通信网络技术手段,把相关资料共享到不同的医生护士、科室与部门等,在方便病患就诊的同时,也可以增强医院管理能力与提升管理水平。

1.2网络安全的概述。基于信息化时代的网络安全对于社会大众的正常生产生活影响非常大,其甚至关系到国家安全与管理。所以新时代的民众都需要了解网络安全的内涵及其特征。网络安全是利用先进的科学技术和不同措施,对有关网络系统的数据资料安全实施保护,防止其被遗失。其具有可用、可控、可审查以及完备等特征。现阶段危害网络安全的原因比较多,比如自然原因(水灾、地震等)、人为原因(人为失火造成的灾害、不法人员制造病毒和黑客攻击行为等),所以必须结合相关原因,采取有效措施开展安全维护。

2 医院信息系统网络安全现状问题的分析

2.1网络安全现状。目前随着互联网技术在社会不同领域的普及应用,使得信息系统已然在现代医院得到充分运用。现代医院信息系统管理的从业人员都会采取不同技术措施开展网络安全防护,比如建立防火墙、采买安全软件、设置病毒检查与防范系统等,上述技术措施可以防控大部分的网络安全。然而基于信息技术的持续进步,使得威胁网络安全的方式方法越来越多且复杂多变。并且由于医院数据资料的重要程度,以及不法人员与域外势力长期威胁着医院信息安全等现状,所以医院信息系统面对的网络安全现状呈现非常严峻的态势,因此医院信息系统管理的从业人员需要结合其运行实际,采取相应的技术措施做好网络安全维护,从而保证医院正常运营。

2.2存在的主要问题。主要体现在：第一,软硬件设备问题。医院信息系统在长时间运行后,会存在系统反应迟钝、经常死机与断网等现象,相关的医护使用者缺乏软硬件知识的掌握,未能即时进行修复,只能待信息系统管理维护人员来修理(由于医院信息系统涉及的软硬件设备多,实际运行时,维护人员都会处于忙碌状态),这种情况将会严重影响网络安全,并且威胁到病患就诊治疗。而且信息系统中的采买软硬件设备资金不足(医院资金主要是应用在药品与医疗器械的采买),影响到医院信息系统及其设备未能得到更新,从而导致网络安全存在隐患。第二,资源配置不恰当问题。医院信息系统网络资源存在不恰当的配置问题,比如医疗和医技在网络资源分配不恰当,使得资源未能得到有效使用,尤其是影像部门的照片量大,其需要的储存资源就要求比较多,这种网络资源配置不恰当现象,制约了重要数据资料的安全保护,所以网络资源配置的不恰当(比如网络方面的服务器资源等)会对医院信息系统的网络安全构成严重威胁。第三,服务器方面的问题。服务器的安全可靠是保证医院信息系统网络安全的关键环节。这方面的问题主要表现为服务器的补丁没有做好修复工作及其弱口令问题,给破坏分子留有可乘之机。并且一般黑客或域外势力的侵袭主要对信息系统网络安全的关键设施开展,造成整个医院信息系统未能正常运行,不仅危害到病患诊治与网络安全,还会损害到医院的经济利益与信誉。第四,制度不完善方面的问题。这类问题一般体现在医院信息系统网络安全管理过程中,安全管理作业标准与作业流程不完善,病毒检测标准与流程。比如文档安全管理标准、入网设施安全作业流程等方面,并且未能对其设施进行全方位的检测等。

3 医院信息系统的网络安全维护措施

3.1结合实际优化网络资源配置的安全维护。网络资源配置需要结合医院经营实际,对其进行合理配置,包括数据储存和网速要求等方面。比如医院信息系统中的PACS与LIS等子系统,可以对其配置高速率的VLAN区域；一般医疗区域,配置中速率的VLAN区域；就医院办公场所而言,其可以配置普通网络速率的VLAN区域,同时可以接入无线网络,确保医护人员与移动医疗设施使用的网络要求。

3.2加强软硬件设备管理的安全维护。结合医院信息系统的实际运行状态,依据医院资产管理的相关条例,结合设备的性能、经济性以及应用要求,做好老化设施的替换工作,确保软硬件设备运行时的网速与网络安全。(1)硬件安全维护管理。医院信息系统网络安全的硬件设施一般包括服务器、机房、网线等,其安全维护管理目的是保证其可靠运行以及防止其发生故障。在安全问题的原因一般是设施老化以及自然灾害影响(水灾、雷电等),因此在安全维护管理时,需要结合不同原因,做好检测工作。同时结合相关设备的安全管理特点和实际状况,采取对应的

文章类型：论文| 刊号（ISSN）：2972-4007(P) / 2972-4015(O)

技术措施，比如安装保险设备。如果是硬件设施老化现象，就有可能影响网络信号强度，因此需要对其进行替换，以达到信息系统网络安全运行目的。(2)软件维护管理。医院信息系统一般包含数据库、传输和操作系统等软件。医院信息系统软件是域外势力和黑客侵袭的重点，其被侵袭将严重威胁到医院产生的各种资料安全。实施软件维护管理工作，首先要运用最新的病毒检测系统，建立健全防火墙，并对其发现的病毒实施查杀，确保网络安全维护管理成效。同时需要及时升级修补软件系统，了解其有可能存在的网络安全风险，做好医院数据资料的储存与处理工作，对医院的重要数据（比如医学科研档案资料等）实施高规格的加密手段，以确保医院信息系统安全。

3.3服务器的安全维护。基于服务器对于医院信息系统网络安全的重要性，其安全维护工作非常关键。规定时间对医院信息系统服务器的不同传送设施开展安全维护（比如交换器、路由器等），具体安全维护内容包括清洁不同设施主板的尘埃，采取措施做好抗氧化工作等等；此外结合该系统的运行实际，采取相关技术措施，做好服务器的补丁的修复工作以及确保服务器是强口令形式，从而保障医院信息系统的网络安全。

3.4病毒防范的安全维护。病毒是黑客与域外势力侵袭医院信息系统网络安全的主要手段，其安全防范措施一般包括：第一，对医院信息系统的内网和外网进行分隔，同时应用相关系统对其实时检测与查杀，防止病毒侵袭问题；第二，制订相关防范制度，及时对其实施检测医院产生的数据资料，运用先进设备和技术措施，增强防火墙运行速率，以保障系统运行安全；第三，依据相关要求，做好数据的加密工作，比如字段加密要求、动态管理密钥等，同时要结合实际状况完善加密形式，从而保证医院信息系统网络安全。

3.5严格访问限制的安全维护。限制访问主要是防范人员因素影响医院信息系统网络安全。第一，严格访问时间的设定，确保访问人员相关资料的准确（比如访问人员的职责及其工作时间等），并且必须动态调整访问人员权限（比如工作时间或工作内容变更等）；第二，严格访问人员的认证。结合医院经营实际，合理选用认证方法，比如利用生物技术对其实施辨认等；第三，严格访问人员携带设施入网的限制，一般采取访问人员的名字、口令与权限对其进行入网辨别，同时对访问人员入网的空间、时间进行监控。此外必须通过加密技术措施，严格访问人员的账号管理。

4 结束语

综上所述，医院信息系统包括医院运营过程中产生的绝大部分数据资料（比如病患就诊资料、科研档案资料以及财务数据等），其可靠运行，可以做好相关的数据处理工作，并且能够在提升从业人员工作效率与医院管理效率的同时，加强不同科室、医生护士以及不同部门与单位之间的联系。但是医院信息系统运行涉及到互联网等相关技术，所以其存在不同的网络安全风险。因此为了保障医院信息系统运营安全，规避相关资料外泄与遗失，以及提升医护工作效率与增加医院管理效益，需要结合其运行现状问题，提出了加强软硬件设备管理、结合实际优化网络资源配置、服务器、病毒防范以及严格访问限制等安全维护措施，从而使信息系统在医院运营中应用的价值得到合理呈现。

[参考文献]

[1]杨晓.医院信息系统的网络安全管理与维护分析[J].中国信息化,2019,(12):73-74.

[2]侯均,王野平.试析医院信息系统的网络安全管理与维护措施[J].网络安全技术与应用,2020,(12):156-157.

[3]程鹏.医院信息化建设中计算机网络安全管理和维护[J].国际公关,2020,(08):204-205.

[4]容甘泉.医院信息系统的网络安全维护探讨[J].信息与电脑,2021,33(06):236-238.

[5]赵昱.新时期医院信息系统的维护和网络安全管理[J].中国新通信,2021,23(18):128-129.

[6]魏玮.医院信息系统的网络安全与维护[J].计算机与网络,2021,47(01):53.

[7]吴兵.医院信息网络安全管理与维护策略[J].电脑知识与技术,2021,17(11):51-53.