医院信息化建设中网络安全及防护的探析

程学波
淮安市第四人民医院，江苏 淮安 223000

[摘要]近年来，我国加大了对外改革开放的力度，从而为各个领域的发展壮大带来了诸多的机遇，为我国社会经济和科学技术的发展起到了重要的影响作用，促进了信息化技术整体水平的显著提升，并且被人们运用到了诸多领域之中取得了良好的成效。但是在信息化技术在加以实践运用的过程中，因为会受到外界多方面因素的影响，所以会遇到诸多的困难。为了满足社会发展的实际需要，各大医院都在积极的落实信息化建设工作，从而使得很多医院内部业务系统逐渐的增加，这样就对网络信息管理工作的实施造成了诸多的困难，这样就对医院信息安全工作的实施形成了诸多的威胁。鉴于此，这篇文章主要围绕医院信息化建设中网络安全和防护展开全面深入的研究分析，希望能够对我国医疗事业的未来良好发展有所帮助。
[关键词]医院；信息化建设；网络安全；防护
DOI：10.33142/sca.v4i2.3828 中图分类号：TP3;TN9 文献标识码：A

Analysis of Network Security and Protection in Hospital Information Construction

CHENG Xuebo
Huai'an No. 4 People's Hospital, Huaian, Jiangsu, 223000, China

Abstract: In recent years, China has increased the intensity of reform and opening up, which has brought many opportunities for the development of various fields, played an important role in the development of Chinese social economy and science and technology, promoted the significant improvement of the overall level of information technology, has been applied to many fields and achieved good results. However, in the process of practical application of information technology, because it will be affected by many external factors and will encounter many difficulties. In order to meet the actual needs of social development, the major hospitals are actively implementing the information construction work, which makes the internal business system of many hospitals gradually increase. This has caused many difficulties to the implementation of network information management work, which has formed many threats to the implementation of hospital information security work. In view of this, this article mainly focuses on the network security and protection in the hospital information construction, hoping to help the future development of Chinese medical industry.
Keywords: hospital; information construction; network security; protection

引言

在科学技术快速发展的影响下，网络技术逐渐的被人们引用到了各个领域之中，对社会的发展和民众的生活造成了巨大的影响。但是因为网络规模的逐渐扩展，从而使得网络系统整体复杂性不断的提升，从而导致网络安全问题越发的凸现出来，对社会和谐稳定发展造成了巨大的限制。

1 医院信息化建设中存在的网络安全风险分析

1.1 威胁分析

在医院信息网络中所涉及到的安全威胁主要牵涉到：病毒的威胁。无线网络遭到攻击或者是钓鱼。高级威胁问题十恶的严重，外部网络连接受到诸多的阻碍，内部身份盗用等等[1]。

1.2 脆弱性分析

医院面临的脆弱性问题主要包括：主机安全管控不足，且医院应用 HOOK 行为较多的特殊性；重要应用系统代码缺陷；操作系统自身存在的脆弱性；信息安全管理制度不完善；信息化管理人员责权不清等。

2 医院信息化建设中网络安全防护的必要性

就现如今实际情况来说，医院信息化建设工作得到了全面的实施，自助付费以及自助挂号等众多先进的科学技术被引用到了医院内部运营系统之中，有效的提升了病人就诊的效率，促进了医院服务整体水平的提升，扩展了医院的各项效益，为医院发展战略的实现给予了良好的帮助。但是，这些项目都涉及到病人和医护人员的信息数据，所以如

果网络系统出现任何的危险，那么必然会造成病人和医护人员的信息泄露，这样就出现了侵犯病人和医护人员财产和个人私隐的情况，对医疗事业的未来良好发展势必会形成诸多的限制。在进行医院信息化建设工作的时候，应当重视网络安全防护工作的实施，这样不但可以切实的对医护人员以及病人的隐私加以保护，并且对于医院树立良好的社会形象也能够起到积极的辅助作用。完善的医院内部网络系统是确保医院信息化建设工作全面实施的重要基础，并且也是医院稳定健康发展的关键措施[2]。

2 医院信息网络安全的关键内容

3.1 信息软件安全

就现如今实际情况来说，医院在实际实施网络信息化建设工作的时候，首先需要组织相关工作人员进行专业技能操作以及理论知识的学习，这样才能保证后续各项工作能够按照既定的计划有序的开展。但是当前很多的医院所使用的系统都是网络终端，在整个网络系统之中，涉及到：电子病历、护理工作流程、药物使用规范标准等多方面内容，虽然可以有效的缓解医护人员工作压力，但是因为利用网络模式来实施病情的诊治病人数量较多，所以会造成网络信息传递时间延长，从而无法切实的对医护人员工作的效率加以保障。

3.2 网络硬件安全

网络安全与存储设备安全二者都是借助电子设备来实施运用的硬件设备，如果想要对硬件设备的安全运行加以保障，确保计算机能够始终维持在稳定运行的状态，那么还需要专业工作人员从多个不同的角度对其进行维保和检查工作[3]。

4 医院信息化建设进程中面临的困境

4.1 人为问题

首先，医院对于网络安全的重要性缺少正确的认识，并没有设立专门的网络安全保障部门。医院内部网络系统安全管理工作往往都是由其他岗位工作人员担任，网络安全工作整体效果较差。如果医院内部网络系统运行出现任何的安全问题，通常都是需要人为进行解决的，但是因为网络安全专业人员较为欠缺，所以无法及时高效的对问题加以解决，这样就无法将网络安全管理工作的作用切实的发挥出来。再有，医院并没有针对网络安全制定完善的规章制度，医院网络安全工作规范性较差，从而造成了网络安全检查和检查工作不能实现既定的效果目标[4]。

4.2 技术问题

通常来说，医院网络系统都是由多个分支基础设施组合而成的，我国医院信息化建设工作发展相对较为滞缓，再加上不具备良好的实践经验，所以在网络安全管理工作实施的过程中，经常会出现系统维护、系统检修、物理环境以及操作系统等多方面安全性问题。经过分析我们发现，造成上述问题的主要根源就是防火墙所拥有的防御功能实用性较差，针对网络旁路以及内部攻击的控制能力相对较差，无法有效的规避网络危险情况的发生，通常只可以起到对攻击行为的预报或者是锁定用户实际 IP 地址的作用。因为国内很多的医院对于 MAC 与 IP 地址管理工作缺少基本的重视，相关工作人员可以随意的更改地址信息，尽管形成的信息内容极易被修改和盗取，并且也无法准确的判断责任人，对于防毒软件来说，因为医院主机数量较多，主机使用人员并不固定，所以无法保证能够对医院所有的主机进行定期的杀毒，这样就造成信息网络安全整体效果较差的不良后果。

5 医院信息化建设中网络安全与防护技巧

5.1 严格执行网络分区分域建设与管理

要想切实的对医院内部信息系统的安全性加以保障，可以结合国家等保 2.0 网络安全等级保护的相关标准在实施各县工作的规划和安排，针对不同功能情况的安全要求保护对象进行区分对待，结合保护对象的设计情况以及安全级别的安全区域，以不同种类的区域重要程度来执行不同程度的安全管理。医院信息系统涉及到生产、办公以及开发测试等多方面内容，应当遵从各类业务的不同情况和特征，将信息系统划分为多个分支系统，随后为各个分支业务系统设计不同的保护级别。信息系统可以说是等级保护管理中的核心内容，为了能够从根本上对网络安全加固保证，切实的对信息安全建设给予辅助，完善信息安全资源配置等级保护，在实施信息系统建设和划分的时候，应当对下列几方面加以重点关注：

5.1.1 管理部门相同的

信息系统中涉及到所有的分支系统往往都是被同一个管理部门进行控制的，并且所采用的安全管理策略都是一样的。

5.1.2 业务类型相似的

信息系统内各个分支系统如果业务类型保持良好的类似性，那么安全需求也存在一定的类似性，所以也可以利用

一样的安全管理策略。

5.1.3 物理位置相同或运行环境相似的

信息系统内所有的分支系统如果物理位置方面或者是所处环境条件都存在类似的情况，那么系统所需要应对的安全威胁也是一样的，在实践中可以选择相同的安全保护措施。

5.1.4 安全控制措施相似的

医疗信息系统中所有的分支系统如果所需要解决的安全问题存在类似性，那么在实践中也可以选择类似的安全控制方法来对业务分支系统的安全性加以保障。结合医院信息系统的业务综合情况，结构特征以及业务系统运行的安全需要，可以将网络划分为多个不同的分支，诸如：医院办公外网、医院业务外网、医院办公内网。这样做也可以有效的提升安全控制工作的整体效果和质量，从而能够确保网络系统在稳定的运行的前提下，切实的增强整个网络系统的安全性，尽可能的规避网络信息丢失或者是泄露的情况发生，为后续各项工作的实施给予良好的保障。

5.2 引入企业级桌面杀毒软件

要想切实的对医院网络的安全性加以保障，那么最为重要的就是在网络防御系统中尽可能的将杀毒软件的作用加以利用，并且还要积极的做好漏洞的扫描、修复以及控制病毒入侵的工作。诸如：可以安装奇安信天擎企业版杀毒软件，利用软件所具有的防病毒以及反间谍软件技术，综合整个网络系统的特征来对网络的安全性加以保障。其次，还需要加大力度的对终端用户进行定期的巡检和管控，这样才能从根本上保证整个网络系统的安全，并且将网络的综合能力加以提升[5]。

5.3 缩小暴露面

5.3.1 缩减网络边界

对于那些在实践中不使用的系统应当尽可能的进行清除，无法在实践中加以使用的功能也应当进行卸载，这样就可以有效的控制访问的范围。在实践中应当对所有的软件的功能加以全面的了解，并且判断其中是否存在隐形风险，在保证安全的前提下加以实践运用。

5.3.2 梳理缺陷资产

资产维度梳理：互联网资产、分支机构资产、外联公司资产、公有云资产；资产属地梳理：特别关注资产的安全属性，中间件或框架（版本）、开放在公网 API 接口（特别是未下线的老接口）、管理后台开放在公网、高危功能（文件上传点、短信验证码、重置密码、文件下载）、远程接入点（VPN）、特权账户（应用管理员特权账户、应用连接账户、系统管理员账户、可以修改账户权限的账户、备份账户）；忽视点梳理：所有内部文档服务器上（含 OA、邮件系统等）敏感信息清理或限制访问权限。

6 结语

总的来说，对于医院信息话建设工作中网络安全信息的防护工作的实施应当加以重点关注，并且结合实际情况和需要来制定切实可行的医院安全管理机制，创设高水平的安全管理团队，加大力度对各类硬件设施进行全面的管控，创设网络安全防护机制，这样就可以对医院内部的病人和医护人员的各项信息数据进行统一的管控，并且促进医院管理工作整体水平的不断提升，尽可能的规避发生医院信息系统被侵入，信息数据丢失或者是泄露的情况发生，从而对医院和病人各项权益加以保障。

[参考文献]

[1]肖军.医院信息化建设中网络安全及防护的探析[J].中国设备工程,2021(2):38-39.
[2]周凯.试论医院信息化建设中的网络安全管理与防护[J].科技创新与应用,2020(34):193-194.
[3]王剑.医院信息化建设中网络安全保护分析[J].科学技术创新,2020(22):92-93.
[4]陈耿杰.医院信息化建设过程中的网络安全防护[J].科技风,2020(20):84-90.
[5]张文玲.探究医院信息化建设中网络安全防护的对策[J].电子世界,2020(13):193-194.

作者简介：程学波（1982.9-），男，苏州大学，本科学历，中级工程师。