现代医院网络安全管理面临的挑战和对策

马 益
广西壮族自治区南溪山医院 广西 桂林 541002

摘 要：面对网络安全的新挑战，我们要深入把握网络安全的基本特性，如整体、动态、开放、相对、共同等，要及时掌握行业发展动态，严格执行国家有关信息安全的各项规定，在做好常态化疫情防控工作的同时落实全面的网络安全保护需求，随着形势的变化而不断地调整防御策略，以更加开放、包容的姿态来增强网络的安全沟通和经验借鉴。传统安全运营模式所体现出的问题可以通过缩小网络暴露面、通过改进新技术新策略，加强安全运营的常态化手段，充分利用外部资源，实现安全运营。

关键词：现代医院；网络安全；管理对策

引言

医院网络安全管理包含多方面的实践工作组成部分，医院网络系统的运行维护工作需要达到常态化的开展实施程度。在智慧医疗的发展宗旨思路指引下，现阶段的医院机构部门都建立了日益完善的网络体系结构，因此有助于医院信息资料得到更高层次的安全监管保护。在现阶段的实践工作开展进行中，医院机构部门的管理负责人员要深刻认识到医院网络安全监管的作用，不断致力于网络安全的监管实践力度强化。

1 医院网络安全发展形势

随着医院的信息化建设的不断进步，利用互联网、物联网等信息化手段进行“智慧医院”、“数字化医院”的转型为医院管理和病患就医提供了很多便利，但也同时也带来了信息安全方面的隐患，针对医院的网络安全防护工作也更加得到重视。网络安全一般是指保护计算机和网络资源的安全和信息不受自然和人为有害因素的威胁和危害，其本质就是信息安全。

从广义上讲，任何与互联网上有关的信息的保密性、完整性、可用性、真实性、可控性等方面的技术和理论，都是需要深入探讨的问题。从医院的角度来说，网络的安全性是基于传统的信息系统的可用性，也就是商业系统的连续性[1]。

目前，针对医院的网络攻击主要是指人为破坏或者有目的性的信息窃取，通过恶意代码、木马、恶意程序等网络攻击，导致网络不可用，应用程序受损，数据完整性受损，主机或服务器受到控制。甚至业务中断，服务器被勒索的安全事故。随着疫情防控措施的不断加强，做好信息化支撑工作对保障医院业务正常运行尤为重要，对医院网络安全也提出了更高的要求。

2 医院网络安全管理的必要性

2.1 保障医院医疗工作的顺利开展

医院各项医疗工作如果想以全面的顺利实施开展，那么关键性的保障技术手段就是维护网络信息的完整性。在智慧医疗的举措深入推进过程中，医疗机构要应对非常激烈的医疗行业竞争。医院网络中的基础数据资料如果失去了安全保障，则会明显阻碍医院正常开展医疗实践业务，并且还会给医院的日常管理活动增加较多的障碍[2]。由此可见，要想确保医院各项医疗业务正常运行，就要建立在医疗数据资源获得安全保护的前提下。

2.2 避免医护人员以及患者的隐私信息泄露

医院科室的医护人员档案资料信息要得到妥善的加密管理，杜绝泄露医护人员个人资料的不良后果。医院网络的安全管理基本宗旨就在于切实维护患者的隐私安全，同时还要保障医院医护人员的合法人身财产利益，防止医护人员档案或者患者的影像病例资料等网络信息被盗取。例如，电子病历也叫计算机化的病案系统或称基于计算机的患者记录。它是用电子设备(计算机、健康卡等)保存、管理、传输和重现的数字化的患者的医疗记录，取代手写纸张病历。它的内容包括纸张病历的所有信息。

3 现代医院网络安全管理面临的挑战

3.1 医院防护资源不足

从医院的发展情况来看，由于医院的特殊性，其安全防护资源存在一定的缺乏，安全防护人员以及技术手段等都存在一定的不足，并且一般比较重视传统的网络安全建设，更多的是注重常规化的安全管理和购买安全产品。自疫情爆发以来，传统的网络安全防护手段已经难以应对目前的网络安全防护需求[4]，并且就医院而言，更加注重的是自身的医疗水平，在一定程度上就导致难以调用足够的资源去培养一批拥有更高技术水平的的安

全人员去应对新形势下的网络安全运营需求，难以应对更新型的网络攻击手段。

3.2 软件漏洞

一切电脑操作系统及其软件管理系统难以避免会有各种各样漏洞和缺点，但这些漏洞很容易被外界非法工作人员故意利用，造成医院中的很多机密信息被泄露，对病人和医院权益导致严重危害。通过对比得知，可能出现协议书等方面的漏洞、动态口令进攻漏洞及其缓存地区外溢漏洞等，而各种各样漏洞生成机制也存在一定差别，会系统产生差异危害，威协医院系统软件稳定运作。

4 现代医院网络安全管理对策

4.1 设置防火墙

防火墙技术也是网络安全中的基础性技术，通过防火墙技术的应用，可在计算机系统的使用中，实现内网与外网之间的隔离，用户在操作计算机系统时，防火墙发挥安全屏蔽作用。数字化医院的防火墙技术应用中，应注意访问策略设置问题，所以操作与使用人员在设置问题之前，需了解自身所接触的计算机信息系统在医院工作中的作用，只有在此基础上，才能保障防火墙技术的作用发挥。防火墙技术的应用中，不仅需保障内网运行的稳定性，更需要尽可能减少外网对用户造成的负面干扰[5]。在医院内的防火墙技术应用，实现对信息系统中各种数据的保护，防火墙技术应用是否得当，关乎医院员工使用计算机系统时的安全性，管理者要针对数字化医院的网络安全要求，由专业的技术人员进行防火墙技术的选择，以通过防火墙，使医院内网免遭非法行为入侵。

4.2 优化并完善安全技术

疫情爆发以来，已经逐渐转变为常态化防控，在这种形势和政策的推动下，物联网、云计算技术越发重要，这种新技术在现代化社会中已经逐渐大量应用起来，这些技术的应用给社会和生活带来了极大的便利。在医院中，随着医院信息化的不断建设，物联网技术和云计算技术也同样被大量使用，这些新兴的科学技术在给医院带来数字化便利的同时，网络安全防护方面需要引起高度重视，针对物联网技术以及云计算技术，需要加强集中资源区域边界的防护，实施最严格的边界防护措施，同时加大在认证、授权方面的技术措施和管控强度，完善技术策略。跟踪安全技术的发展，并适时引进新的安全产品。

4.3 加强对网络信息安全的防护能力

医院对其数据和信息做统筹管理时，必须提升网络信息化管理工作的安全防护能力，因此，医院应加强基本建设网络安全人才团队投入幅度，这也是维护保养网络安全的关键工作。网络安全团队是为了维护医院网络安全安全防护工作中而活着，因此这一点在其经营范围以内，也是其工作职责。安全性团队的品质、工作中能力、综合能力、危机意识对医院网络安全安全防护工作中的效果拥有极为重要的选择功效。在规划医院网络安全人才队伍管理时应注意二点具体内容，即高质量人才的引入和培养具备有关安全防护知识的人才，仅有从这两个方面下手才能够进一步确保应用系统更具有安全系数。在如今这一人才竞争白热化社会发展大环境下，医院招人时能设对应的职位职责关键点、必须的薪资福利及其比较有限名额的岗位晋升等政策，可最大程度地吸引人才，还可能吸收大量有着高质量、高专业知识的优质人才[6]。从员工塑造方面来看，医院能选与更专业的网络安全部门进行协作。一方面，医院可以利用她们先进技术与最新管理模式去培养医院网络安全管理方法人才；另一方面，也能有效提升医院网络安全安全防护的内部能量，当医院发生紧急状况时他们能够给予一定的支援，这进一步保证了信息化管理互联网的安全性。

4.4 完善落实管理制度体系

新时期下的医院信息安全建设应以信息安全对策为载体，以员工管理为依托，以信息安全管理方案为核心，紧紧围绕医院信息内容网络构建全方面的信息安全管理体系。在制度体系层面，必须做到主要领导亲自抓，不断完善信息安全工作规范，积极开展信息安全自纠自查工作中，确保诊疗业务流程的优良运作，保证信息管理系统的安全性。每个部门一同商议，对安全性管理的必要性达成共识，同时结合部门职责建立和完善的制度体系。在安全管理层面，应塑造整体、全局性网络安全担当意识，重视医院统计数据的个人隐私保护，强化对全体员工的网络安全文化教育。特别是在应塑造对于钓鱼邮件、故意网页页面、明文密码设定等典型案例的安全防范观念和能力塑造，减少因为安全防范意识和能力不够所带来的网络安全安全隐患[7]。在医院信息安全管理方面，明确职责范畴、划定义务地区，保证任何工作人员清楚自已的安全管理。

4.5 加强网络安全应急响应建设

根据医院以往的发展规划和信息安全投入情况来看，在网络安全应急响应方面的建设其实是不足的，当发生紧急的网络安全事件时，无法及时、有效的去处理这些安全事件，就医院这个网络安全建设情况来看，其信息安全人员的网络安全反应能力直接影响到医院的核心资产的安全。建立快速、灵活的网络安全监控、预警、研判、决策、处置、追溯和报告机制，加强联系、

调度和流程平台的建设，制定健全的安全事故处理方案，规范应急指挥程序，强化网络安全应急反应程序，加大自身在网络安全应急响应方面的能力建设投入，保障医院网络高度安全和可靠。

4.6 健全网络安全防范机制

在医院网络安全安全防护工作上，不仅需要提高医护人员安全防范意识，还要进一步完善医院网络安全预防管理体系，提高医院网络系统的牢固安全度。例如，进一步加强医院网络系统基本建设，合理布局软硬件建设，为医院进一步优化网络安全系统软件打下良好基础；利用有效引进各种各样管理心得和安全生产技术，确保网络安全运作；对网络数据数据信息执行备份数据解决，对各类安全保密性文件传送必须做好验证数据加密，框架电子计算机网络防火墙，有效使用各种各样杀毒软件，做好医院网络系统日常管理方法日常维护工作。医院网络相关安全防范是一种长期性、系统软件、繁杂的工作中[8]。对其医院网络安全执行综合性安全防护环节中，必须对于网络安全风险性制订完备的安全防护规章制度，在日常活动中标准具体指导医护人员具体步骤个人行为，对于不同职位单位贯彻落实网络安全风险管控岗位职责。因此，必须医院联络本身具体发展情况和行业整体转变局势，制订达到自我发展必须的发展战略，并且具有一定高效性和合理性的风险管控管理体系。

4.7 合理创建专区专访控制功能

医院网络安全安全防护过程中需要灵活运用专区专访操纵作用。医院在建立网络系统架构设计中，必须确保医院内部结构网站访问的靠谱安全度，在这种环境下能够灵活运用专区专访作用。在实践过程中，必须进一步揽活浏览有关管理权限特点，把内部网进一步定义成多种多样作用VLAN，办公场所产生不一样业务流程PC终端设备，关系客户身份证信息，对有关访问限制执行科学合理设定，客户进到互联网后，可以通过本身范畴管理权限，进到特定网络服务器及其互联网区域。依靠以上方法，相匹配信息内容浏览全过程就会更为稳定性和安全性，适用医院网络系统进一步改革创新[9]。医院必须建立完备的安全性信息化管理自然环境，有效操纵医院里外网络安全难题产生。因此，医院可以利用侵略监测系统、数据加密、网络防火墙及其密钥管理技术性建立安全防护系统。互联网信息安全防护工作人员要做好医院网络数据的监管与文物保护工作，为医院成功开展互联网数据交换平台给予相对性靠谱、平稳室内环境。

4.8 加强安全监管力度

医院管理人员针对网络硬件以及网络软件系统都应当展开安全监管维护，定期实现针对网络硬件的基础设施更新处理。医院员工以及管理者对于患者个人的病例信息以及影像资料等需要进行妥善的安全保存，切实维护医院数据库的完整安全性。患者个人隐私有关的资料信息都要保存在指定的医院网络系统中，避免患者的隐私数据信息存在泄露的安全威胁因素。医院应当着眼于以患者为本的基本实践工作思路，积极运用信息化的智能技术手段来维护患者的个人隐私安全，提升患者的服务满意程度。

结束语

总的来说，在医院互联网不断深层次建设发展趋势环境下，面临的安全隐患难题更加明显，而医院网络风险的应急处置工作也成了医院新形势下建设发展中密切关注具体内容。因此，医院和相匹配工作员必须深刻认识到医院网络安全防范重要作用，在充分提高自身网络安全意识前提下，挑选有效对策科学解决，确保医院网络信息系统的安全性、平稳运作。

参考文献

[1]赵现,王力华.医院网络安全管理中心建设初探[J].中国数字医学,2021,16(02):117-120.

[2]徐航.探讨医院信息化建设中的网络安全管理与防护[J].科技风，2021（13）：109-110.

[3]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.

[4]周润.信息化背景下医院网络安全管理措施研究[J].科技资讯,2020,18(18):26-27.

[5]董晓非.医院网络信息安全的防范技术探讨[J].信息记录材料，2020,21(2):2.

[6]沈志伟.医院信息化建设中网络安全管理与防护的探讨[J].无线互联科技,2021,18(22):33-34.

[7]陈晨,包曾.医院网络安全管理体系的建设方法分析[J].网络安全技术与应用,2020(08):128-129.

[8]金扬.医院信息化建设中计算机网络安全管理与维护[J].智能城市应用，2021,4(6):3.