数字化医院计算机信息网络系统安全及对策

姜柏旭

吉林省吉林市人民医院　吉林　132001

[摘　要]当前，医院逐渐向着数字化方向发展，很多医院都纷纷开始在管理工作中引入了计算机信息网络系统，但是在诸多因素的影响下该系统的应用还存在诸多问题，严重阻碍了医院的良好发展。鉴于此，本文将对数字化医院计算机信息网络系统安全及对策展开探讨。

[关键词]数字化医院；计算机；信息网络系统；安全；对策

【DOI】10.12252/j.issn.2096-627X.2020.03.024

1 数字化医院概述

现阶段，数字化信息技术被广泛运用于数字化医院建设过程中，数字化医院计算机信息网络系统的特点在于使用时间长，为了保证该系统能稳定运行，需要保证信息网络系统的安全性和稳定性，而计算机信息网络系统在运用的过程中会出现一些难题，从而影响数字化计算机信息网络系统管理的有效性，因此需要做好数字化医院计算机信息网络系统的安全管理工作，同时还需要保证信息传输的安全性。数字化医院有着十分重要的意义，建设数字化医院可以实现社会向信息网络的构建，同时能加强医院和上级部门、护理人员和病人等的联系，以此来提高医院管理的规范性和有效性。数字化医院的建设能提高医院运营的智能化程度，主要表现在于数字化医院模式之下医院的工作方式实现了升级和转变，在这个过程中可以实现传输医学影像网络和结果，提高社会资源利用的效率和质量，同时还可以有效提高医疗数据的同步性，以此来提高医院的服务质量，为患者提供更好的服务。同时，在数字化医院的模式下，开展工作的过程中可以实现医务人员和网络及远程操作之间的连接，从而推动医生工作性质的转变，加深医务人员与人才管理中心等部门的合作。

2 数字化医院网络信息安全问题

2.1网络安全管理问题

目前，一些医院传统管理意识比较根深蒂固，而且欠缺先进的管理手段，所以不利于医院网络安全管理工作的顺利进行。在实际上，一些医院过于注重提高医疗服务水平，并没有对医院数字化建设予以高度重视，由于医院领导和管理人员思想意识的薄弱化，所以网络安全管理水平始终停滞不前，其管理手段与当前网络技术要求并不相符，所以安全漏洞在医院网络系统中始终没有得到治理，黑客攻击屡禁不止，从而使医院陷入困境。

2.2技术人员问题

开展数字化医院计算机信息网络系统安全管理工作的过程中存在的另一问题在于，缺乏专业的技术人员，因此无法为安全管理工作提供相应的技术支持。保证数字化医院计算机信息网络系统的安全性能保证整个医院工作的正常开展。而保证计算机信息网络系统的安全性离不开系统内部各个环节的共同运行，如果在系统运行的过程中某一环节出现问题，往往会影响到整个系统的安全稳定运行。现阶段计算机信息网络系统在运行的过程中会受到黑客和木马程序的侵袭，这使得在开展计算机信息网络系统维护工作的过程中会耗费大量的时间和精力，因此需要从源头做起提高技术人员的能力和水平，从而提高技术技术人员应对突发情况的能力，以此来保证数字化医院计算机信息网络安全系统运行的安全性和稳定性。

2.3操作系统安全问题

在医院网络系统中，安全漏洞经常出现，而且在系统运行过程中，其TCP/IP协议的安全隐患同样不容忽视，尤其在授权管理和资源访问等方面，从而使在网络系统运行过程中，节点自行配置现象经常出现，不利于IP协议各节点的统一性和集中化，甚至造成IPSpoofing攻击行为的出现，从而威胁到医院网络系统。此外，在医院数字化建设过程中，OA、HIS等系统得到了广泛应用，虽然可以不断提高医院网络系统运行效率，但是一旦出现安全隐患，极容易影响到网络系统。在应用SQLSev-er、Oracle数据库过程中，安全隐患同样存在，一旦不及时采取措施加以强化，必然会严重影响到医院网络系统的正常运行。

2.4网络边界安全问题

目前，诸多医院在设置内网和外网方式时，往往采取独立性原则来进行，以此来将医院网络系统的安全性提升上来，防止入侵外界网络病毒，以免对医院网络系统造成影响。基于本质视角，对诸多医院数字化建设水平进行分析，初级阶段比较明显，而且一些医院尚未广泛应用IT技术，所以在连接医院内外部网络时，C/S、B/S的模式比较常见，一定程度上不利于医院网络系统的正常运行，而且黑客入侵也经常出现。此外，部分仍然对传统防火墙技术进行应用，所以很难有效防御攻击行为的出现。

3 数字化医院计算机信息网络系统安全对策

3.1预防病毒，重视数据库加密工作

在病毒预防方面，医院可构建对信息网络系统予以操作的具体制度，对信息网络系统涉及的相关注意事项和操作方式进行明确，降低由于人为因素引起的病毒入侵问题。同时，技术工作人员需要对病毒查杀软件予以更新和审计，确保病毒库处在最新状态。除此之外，应给予数据库加密更多的关注，在设置密码的过程中要尽可能运用组合字母、符号与数字的方式，以免密码过于简单，轻而易举便被破解。并在固定的时间备份数据库中的数据，促使因为数据损坏或丢失带给医院巨大的经济损失。因为系统在实际运转的过程中，会出现漏洞，同时黑客擅长借助漏洞对系统进行攻击，所以技术工作人员应对系统存在的漏洞进行及时的修复，有效防御病毒和黑客入侵信息系统。此外，重视对系统的维

护，详细记录系统的运行情况，以便于能够第一时间找到系统在运行过程中存在的问题，确保系统质量，夯实医疗活动有序进行的基础。

3.2实现对信息数据库的及时备份

医院在运行过程中难免会出现停电、地震、海啸等不可抗力的影响，因此，医院数字化计算机网络系统应实时将患者治疗信息进行上传备份，避免这些数据丢失或者人为删减，医院互联网技术人员需要构建信息数据库，并将这些数据定期上传到数据库中，确保数据完整无误。

3.3引入安全防御策略

医院数字化计算机信息网络系统主要是通过对医院业务系统、网络系统、操作系统等系统进行严格的把控，从而做到数字化网络系统的安全性和稳定性。文章主要从系统安全防御、网络安全防御、边界安全防御三部分进行简单概述，具体内容如下：（1）系统安全防御。主要是指互联网信息技术人员通过以医院数字化网络信息技术系统为基本服务对象，在网络信息技术系统中安装相关保护系统，例如：防病毒软件，从而提高网络安全系统防御能力，一旦出现外界病毒入侵及时报警，将医院损失降到最低。（2）网络安全防御。网络安全防御主要是在医院数字化信息网络系统中安装VPN及时和病毒入侵检测系统。一旦外界病毒、不法分子或者未授权用户端强制入侵网络时，VPN技术检测病毒系统将会直接对入侵对象进行检测，从而确保医院数字化信息系统的安全性和可靠性。另外，互联网技术人员在安装VPN技术时，需要对医院数字化信息系统进行检测，在护理位置安装VPN软件，避免出现报警出错现象为医院带来麻烦。（3）边界安全防御。互联网技术人员通过加强医院网络边界安全，从而通过在医院网络中安装防火墙，对不安全网站进行浏览、对非法用户进行筛选、对存在一定危险的账号进行警示，通过利用防火墙来对医院网络存在的危险进行防控，避免医院网络信息系统遭受到病毒、木马入侵，做好医院网络系统防控的一道围墙，实时监管网络信息系统的安全。医院互联网信息技术人员在做到上述三点条件下，还需要对医院网络信息系统的登录密码和用户名进行调整，技术人员需要通过采取加密算法得出系统的登录密码，从而确保登录密码难以被不法分子破解，便于更好的完善医院网络系统的安全性。另外，互联网技术管理人员还可以通过对访问用户权限进行审核，并且适当的授权访问用户一些权限，从而可以更好地为患者进行治疗，医院通过对访问人员采取权限控制的方式从而可以更好地约束医院网络信息技术系统。

3.4实现对数字化医院计算机信息网络系统的升级及漏洞修复

医院信息技术人员需要定期检查医院网络信息网络系统，一旦发现医院网络信息系统出现故障及时采取一定的解决措施。信息技术人员还需要定期对系统进行维护、升级，对医院网络信息系统进行系统的修复，降低外界非法分子入侵概率。另外，网络信息技术人员还可以定期对医院数字化网络系统容量进行扩容，同时将治疗成功出院并且一定年限之内没有就医的患者相关信息拷贝到治疗成功患者的网络系统中，同时将医院数字化网络系统分为两个子系统，避免数据流过大，网络信息系统瘫痪的情况。

3.5提高技术人员工作能力

医院网络系统在实际运行过程中，医院应对计算机技术人才的管理与储备工作引起重视。一般而言，技术人员所具备的能力与医院系统运行之间存在着紧密的联系。对于信息安全而言，技术人员发挥着极为重要的作用，同时也是网络系统维护工作中不可或缺的一部分，确保系统能够维持在稳定、安全的状态中。以此为基础，医院应积极培养技术人才，提高招聘门槛，构建完善的招聘制度，并考核有关人员所具备的计算机操作能力。同时，为了能够提高人才培养效果，员工还没上岗前，医院应切实做好岗位培训工作，加深其对医院网络系统的了解。在网络系统管理维护上，还要积极开展技术能力培训活动，在固定的时间组织课程再培训和进修学习，以促进人才技术能力提升，确保其能够更好融入安全管理工作中，提高系统安全运行水平。

3.6有效评估计算机网络安全风险

当前，在我国网络技术发展中，管理与技术属于对网络安全风险进行评估的主要内容。随着科学技术发展速度的日益加快，对网络安全风险进行评估，属于技术含量极高的一项活动。将管理与技术作为立足点，进行双向综合性评估分析，有效筛选系统中产生的诸多信息，以此对计算机网络之中涉及的风险动向进行全面分析，以便于通过各类评估方式进行安全性总结。除此之外，在使用管理与技术两个方法时，所运用到的途径不同。其中，管理方面重点是展开社会问卷调查，技术则为对安全风险进行全面分析定义。当前，社会上诸多ISS以及NAMP均是运用这种方法展开网络安全风险评估。

4 结束语

基于数字化视角，加强计算机信息网络系统的应用，不仅可以促进医院运营管理的正常进行，践行规范化和科学性原则，有力保证医院各项工作，而且还可以顺应医院现代化发展趋势。但是在医院计算机网络系统中，存在着一些安全隐患，这对于网络系统的安全运行产生了极大的影响，所以应加强安全对策的制定，实现数字化与医院的高效融合，共同致力于医院可持续发展目标的顺利实现。

参考文献

[1]吴亮.数字化医院信息系统集成技术的应用[J].电子技术与软件工程，2018，0（6）：166-166.

[2]丁斌.数字化医院信息系统规划研究[J].无线互联科技，2016，0（4）：49-50.

[3]顾学赛，王梓名.Oracle的DataGuard技术在医院整体数据迁移中的应用[J].现代信息科技，2019，3（13）：162-164.

[4]孟晓阳，朱卫国，李连磊，苏博，张楠，李爱巍，马学泉，黄迎萍.“互联网＋”对医院信息系统安全的挑战与对策探讨[J].医学信息学杂志，2016，37（12）：38-41.

[5]于鑫，刘宏伟.医院计算机网络信息系统的安全问题及对策[J].电子技术与软件工程，2018，0（5）：217-218.

[6]李宏伟.医院计算机网络的发展与医院计算机应用的重要性[J].信息与电脑，2019，0（1）：26-28.