互联网+医疗健康模式下的医院网络安全与防护研究

Research on hospital Network Security and Protection under the Internet + Medical and Health model

王哲 Wang Zhe
中国科学技术大学附属第一医院安徽省立医院 安徽 合肥 230000
The First Affiliated Hospital of University of Science and Technology of China, Anhui Provincial Hospital, Hefei, Anhui 230000

【摘 要】在互联网+医疗健康模式下，医院信息系统的功能进一步扩展，实现网上预约、登记、支付、诊断和治疗。基于此，本文分析互联网+医疗健康模式下医院网络安全隐患，探究网络安全与防护的对策，促进医院实现在线服务的功能，顺利将医院局域网与Internet连接起来进行数据交互，确保网络建设和安全达到标准，高效进行相关业务。

【Abstract】Under the Internet + medical and health mode, the functions of the hospital information system are further expanded to realize online appointment, registration, payment, diagnosis and treatment. Based on this, this paper analyzes the hidden dangers of hospital network security under the Internet + medical and health mode, explores the countermeasures of network security and protection, promotes the hospital to realize the function of online service, smoothly connects the hospital LAN and Internet for data interaction, ensures that the network construction and security meet the standards, and carries out related business efficiently.

【关键词】密码口令；防护框架；病毒预防

【Key words】password password; protection framework; virus prevention

引言：

随着计算机技术和网络技术的飞速发展，医院信息系统不断更新，可处理的业务范围不断扩大，业务管理的内容也在不断丰富。另外医院的工作已从简单的医疗活动扩展到管理、科研、教学等领域，此时医院的信息网络安全就面临着非常大的挑战。

一、互联网+医疗健康模式下医院网络安全隐患

（一）密码口令入侵问题

在计算机网络运行的全过程中，密码口令入侵是目前最常见和最具影响力的安全问题，黑客可以使用穷举法或暴力法破解合法密码和主机账号，从而达到破坏网络安全的目的。通过这种方法，黑客可以登录他人的主机，修改主机上的相关文件，获取用户的合法主机密码和登录账号，从而直接监控和攻击用户的来往信息，这种方法对用户信息造成极大的危害，容易导致用户信息的丢失或被盗。近年来计算机技术不断发展，在此背景下虽然许多医院网络管理员在不断变化的网络环境下设置了相应的访问密码，但有些密码相对简单，就比如 6 个 6、8 个 8 这样的密码，或者用自己的生日或手机号码作为密码，这样的纯数字密码缺乏足够的安全性，使得黑客有机会在医院网络环境下进行频繁的密码入侵。

（二）WWW 欺骗技术入侵

WWW 欺骗技术在当前网络环境下也很常见，这种技术主要是不法分子入侵网站或自制钓鱼网站，通过网络应用诈骗计算机用户或直接窃取用户的财物。WWW 欺骗技术，主要是黑客通过入侵网站，并在网站设置病毒，一旦用户进入网站后下载某些软件或点击某些链接，就会在用户的电脑中植入病毒，用户访问的 URL 可以被黑客作为自己的预置主机来操纵。经过这些步骤，黑客可以直接攻击医院服务器的网络漏洞，也可以入侵医院数据库窃取信息和更改文件[1]。与外部网络连接可能造成入侵风险，互联网医疗模式的目标是为社会和患者提供更有效的服务。为了解客户的需求，医院网络必须连接到外部，例如，在医疗保险结算的情况下，医院需要与医疗保险办公室共享患者信息，并在第一时间更新患者就诊信息。目前医院经常会使用在线预约、在线注册等服务。需要病人自己操作手机软件或银行自助终端，这一现象的背后是医院网络与互联网之间的信息交互。医院网络服务需要与其他网络进行交互和协作，这意味着医院局域网的接入量增加，医院网络被入侵的概率也会增加。

（三）内部因素威胁

密码入侵和 WWW 欺骗技术都是由外部因素引起的风险，而用户在计算机应用过程中也会受到一定的威胁。通过一个简单的分析，可以发现我国 70%左右的医院存在不同程度的内部风险，尤其是公立医院，这一数字达到 95%左右，导致公共医疗资源网络安全问题频发。主要原因是计算机用户缺乏安全意识，在使用计算机时缺乏有效的管理，或者在一些非正式网站上直接下载盗版软件。这种操作可能会导致

某些系统漏洞，从而导致网络安全问题的频繁发生。尽管我国大多数医院都建立了一定的网络防火墙，而且工作人员也有使用网络安全的想法，但仍以主观感受选择计算机的防御工具，没有配置相应的安全程序，这对计算机的安全防御造成了一定的影响。所以，在计算机网络安全管理中，既要注意网络环境的外部攻击，又要注意计算机的内部管理，以保证病人或医院的信息安全。

（四）复杂的用户组成和设备组成

医院网络用户的构成相当复杂，除了进修、实习等医务人员外，还包括从外部聘请的工作人员。这部分医护人员不会长期参加医院工作，通常半年或一年后就会离开，因此很少有医院将这部分人群纳入医院网络信息安全培训人员的行列，大多数医院将这部分人员视为临时人员，不强调安全使用网络，而且不会要求这部分医务人员严格执行医院网络安全规则，所以会出现一系列的非法操作。例如，任意使用个人 USB 盘，这就有可能带来病毒，或未重视信息保护。医院网络复杂，用户数量庞大，医院网络安全无法保证。就目前的医院网络安全系统而言，大部分医院已逐步发展为三层交换网络，不再局限于原来的门诊部，而是逐渐延伸到医院的各个楼层，几乎整个医院都覆盖在内。大规模网络系统需要大量的网络设备、终端设备来支持，因此网络的物理安全、接入设备的安全性成为管理难点，稍有疏忽就会对医院网络造成负面影响。

二、互联网+医疗健康模式下的医院网络安全与防护措施

（一）科学设计网络信息安全防护框架

所谓网络信息安全防护框架设计，是指在网络建设过程中对网络安全体系结构的设计。设计的内容主要是基于数据中心、网络输入输出和终端。就像数据库一样，数据中心服务器和前者都使用企业版的系统安全保护软件，同时备份数据库中的所有数据，对信息的功能进行合理分类，有效提高数据库的安全性。设置好预订的备用线路和服务器，突然停电会造成信息损害，为避免出现这一不良情况，应提前准备好不间断的电源。就网络的输入和输出而言，建立防火墙，制定入侵防御策略，对一些非法访问实现有力控制，并积极实施设备检查输入的相应安全配置，提高设备的安全水平。在各个咨询室、护理站都需要安装企业版本的防护软件，进行有力的终端管理。设置好数据库安全信息的更新时间，禁止使用不属于设备的硬件终端口。降低磁场和热量对时间链数据传输网络的影响，并防止在挂壁式的开关设备端口的乱接线，防止在网络中产生回路，保证网络正常运行。

（二）建立监测和安全系统

安装网络信息安全监测防护设备，对及时监测医院网络和网络设备的安全具有重要意义。实现安全监控系统的配置可以发现安全系统中的异常设备和异常的数据包，从而及时停止所有未经授权的访问。监控数据中心的物理环境，实时了解数据中心机房的温度、湿度、电压和电流的变化，在此条件下，医院信息可以在第一时间传递给服务人员，以避免安全风险事件的发生。强调做好对软件和数据库的保护，以防止医院网络中使用的软件出现安全问题，数据库、所有会诊室和护理站都应配备企业级机构版本的安全保护软件，而且这些安全保护软件应及时更新。医院可以使用的安全软件包括诺顿安全软件、360 安全卫士，病毒防护软件的存在，在一定程度上可以防止木马病毒窃取各种隐私信息。

（三）加强完善网络接入制度

医院网络覆盖范围越来越广，所涉及的信息量越来越大，需要配备的信息终端数量明显增加，此外医院网络的用户数量也在增加。医院网络信息终端需要处理大量的业务活动，管理难度大，管理起来也非常复杂。为了解决这一问题，有必要建立医院网络接入准入机制，用户使用医院网络需要购买临时帐户或对用户进行身份验证，可以实现对临时访问医院网络人员的统一和全面管理[2]。在一定程度上，遵守网络使用的规章制度对医院的网络安全有着深远的影响。因此，有必要完善医院网络使用的规章制度，以避免因使用不当而造成的网络信息安全问题。仔细监督医院终端的接入操作是否符合管理层的安全要求。避免医院网络系统运行过程中发生障碍和问题，只有保证医院网络系统运行的安全性和可靠性，才能有效提高医院办公效率，充分发挥网络在医疗模式管理中的作用。有关网络使用的规章制度，内容很多，除了医务人员使用网络的要求外，还有临时人员使用网络的指导方针和使用方法，用户正确使用网络，进一步提高医院网络使用的安全性。

（四）做好威胁入侵和病毒的预防

流量清理后，仍然存在扫描、嗅探、恶意代码等威胁，这些威胁会通过系统漏洞，规避保护措施，实施系统入侵行为，进而控制主机系统。一旦入侵成功，就会造成巨大的损失。应做好入侵防御系统（IPS）的部署工作，检测并有效防御恶意行为，这些恶意行为可能造成网络和主机的运行故障，此时需要查找特征码，识别过滤有害数据流。基于基本特征的入侵防御系统无法应对高级别的持续威胁，所以在构建入侵防御系统时应特别小心这种攻击损害保护系统，提高系统的态势感知能力，建设可视化系统，监测整个网络的流量威胁[3]。据国际著名病毒研究机构国际计算机安全协会（ICSA）统计，目前只有 7%的病毒是通过磁盘完成传播的，其余 93%主要来自电子邮件，这其中包括了网页、QQ、MSN 等渠道方法，由此可见计算机病毒的发展趋势是网络化。因此医院必须部署防病毒屏障、防病毒网关，以进一步确保网络进出数据的安全性。使用 HTTP、FTP、SMTP、IMAP 等

协议完成对网络病毒的扫描，一旦检测出数据病毒，将采取相应的措施进行病毒分离和杀死，这在保护网络无病毒环境方面发挥非常重要的作用。

结束语：

综上所述，互联网+医疗健康模式下医院网络安全隐患主要是密码口令入侵问题、WWW 欺骗技术入侵、内部因素威胁、复杂的用户组成和设备组成。有效应对上述威胁，应建设网络信息安全防护框架。建立监测和安全系统，加强完善网络接入制度，做好对威胁入侵和病毒的预防。建设严格的网络安全方案，提高医学治疗实施水平。

参考文献

[1]张千彧,邱宾,武甲庚.5G 技术助力“互联网+医疗”健康管理模式发展[J].中国卫生质量管理,2020,27(06):81-84.
[2]于金涛,王晓波.基于互联网+医疗健康模式下的医院网络安全与防护工作探究[J].数码世界,2020(11):197-198.
[3]黄兴文.互联网医疗模式下探讨医院网络安全现状及防护策略[J].信息记录材料,2020,21(04):220-221.