医院管理

新形势下军队疗养院网络安全问题与对策分析

戴 兢,李 敏,万永强,邱榕彬

【摘要】 随着军队信息化建设的推进及编制体制调整改革变化,军队疗养院的网络安全工作迎来了新的难题,面临着更高的要求。文章结合陆军厦门特勤疗养中心情况对军队疗养院网络安全问题进行分析,并从加强人员教育、提高防范意识,加强网络安全管理建设,构建网络安全防范体系三个方面进行对策思考,其中构建网络安全防范体系包含优化网络规划、促进云平台建设、建立网络安全态势感知预警系统。如何立足现有,结合新技术发展,满足新的安全需求,始终是军队疗养院需要探讨的重要课题。

【关键词】 军队疗养院;网络安全;问题分析;对策;云平台;安全态势感知

【中图分类号】 R197.7 **【文献标志码】** A **【文章编号】** 1672-271X(2019)06-0661-03

【DOI】 10.3969/j.issn.1672-271X.2019.06.025

0 引 言

随着军队信息化建设的推进和信息网络的发展,疗养院网络呈现了多样化,信息化设备种类与数量大大增加,网络环境变得更为复杂。疗养院信息系统的功能也日益完善,涵盖了疗养、体检、管理、后勤保障、办公交流等多方面。信息系统的数据种类多、数量大,其中军队疗养员的信息具有极高的私密性,网络安全问题随之日益突出[1]。军队编制体制调整改革后,疗养院新组建为疗养中心,疗区间分散,办公更加网络化,这对网络安全提出了更高的要求。因此,加强网络安全管控、保障网络安全是军队疗养院工作中非常重要的一部分。

1 现状及问题分析

随着人工智能技术的不断进步,军队疗养院建设从过去的数字型逐步向智慧型方向发展,数字化设备种类和数量大幅增多,用户行为越加难控[2],但缺乏相应的安全防范能力。面对随之层出不穷暴露出来的网络安全问题,轻则资源损耗,重则数据泄密、系统崩溃,造成严重影响和破坏。如 2017 年爆发的勒索病毒以及每年频发的信息数据泄密问题,虽然相应的防护策略技术很快发布出来,但对已造成的损失难以挽回。

我院近期多次安全检查中,暴露出在信息安全建设上存在诸多薄弱环节,如经常性基础性工作不扎实,安全管理机制存在漏洞,人员保密意识不强,安全建设技术不完备等问题,现结合我院情况对军队疗养院网络安全问题进行分析。

1.1 人为因素 在信息化时代,网络办公设备的使用普及率非常高,但大部分人员仅掌握业务操作方法,缺乏对网络安全知识的认识。近年来编制体制发生调整,出现大量人员转业、换岗的情况,导致人少事多任务急,一方面人员易产生侥幸心理,为方便简化安全工作流程,另一方面易导致保密安全意识不强,认为疗养院无密可保,为军队疗养院网络安全埋下隐患,使网络安全管理非常棘手[3]。

1.2 管理因素 疗养院作为医疗单位,相较于网络安全建设更加重视医疗建设资源的投入,在网络安全防范工作上往往是上级检查后补漏,缺乏主动性与前瞻性。并且受限于人员编制等问题,大多疗养院紧缺网络安全专业管理人员,而目前管理决策层对网络安全管理与建设缺乏技术理论支撑,易忽视在相关软硬件的投入,易产生网络安全的管理机制不够有效、规范的问题。

1.3 环境因素 疗养院具有疗区建设分散,地理位置多分处山区、海岛的特点,各疗区有部分自己独立的信息系统,也有共用的信息系统,既独立又相互关联,但网络安全建设往往以其中的主疗区为中心,其他疗区易被忽视,出现防范措施传达不到位的问题。由于疗养院的业务性质,通常各科室分散在不同建筑中,导致网络硬件设备数量庞大而分散,同时设备易受自然环境因素影响,如潮湿的环境对硬件设备寿命带来极大的考验,这为网络部署

作者单位: 361002 厦门,陆军厦门特勤疗养中心信息科(戴 兢、李 敏、万永强、邱榕彬)

通信作者: 李 敏,E-mail: 171847712@qq.com

与维护带来难度。

1.4 技术因素 与医院相比，疗养院信息科创建时间短，专业技术人员较少[4]，网络安全维护技术力量一直较为薄弱，网络安全防范技术更新缓慢，应急能力差，监查手段单一落后，不能及时对网络安全问题做出判断和响应。此外，军队疗养院主要使用的业务系统为原沈阳军区大连疗养院 2005 年研发的军队疗养信息管理系统，该系统的更新已难以跟上疗养院的发展需求，系统功能单一且存在较多缺陷。为满足新的业务需求，疗养院局域网内同时运行了十余个系统，如财经平台、OA 办公系统、体检系统、检验系统、绩效管理系统等，各信息系统多由不同的服务商搭建或由上级下发，系统的防护能力参差不齐，缺乏统一有力的网络安全防范体系。而传统的服务器的建设与维护较为分散，存储的数据安全性不高，硬盘的浪费率比较高，增加安全管理的难度。

2 对策及分析

从定义上来看，网络安全是集合工具、政策、安全概念、安全保障、指南、风险管理方法、行动、培训、实践案例、技术等内容的一整套安全管理体系[5]。因此，建立统一的网络安全防范体系需要来自技术、管理等多方面的支撑。

2.1 加强人员教育 人是安全防护体系中至关重要却最薄弱的环节，需要加强经常性的安全保密教育，普及网络安全知识，才能达到有效的网络安全防范。做到一人不漏，人人掌握，强化责任意识，杜绝行为上的随意性，形成良好的办公保密秩序。区分管理层、技术层、基层使用者，从管理制度、专业技能、操作规程等方面有针对性进行分层学习，重点加强涉密岗位、重要值班值勤人员的保密教育和业务培训。

2.2 加强网络安全管理建设 根据军队保密规定以及疗养院实际情况，不断完善网络安全管理制度与工作流程。明确安全管理主管部门、主管人员，科室设立网络安全员，形成全院—科室—个人的三级管理体系，明确各级人员职责、权限、分工。严格网络设备采购、使用及管理规程，加强运维管理，制定网络安全应急响应预案和处置策略，应对可能发生的网络安全问题。信息科应设置专业网络安全技术人员负责网络安全工作，加强专业技能的培训与学习，提高疗养院网络安全防范技术水平。针对现有技术力量不足的问题，加强信息化人才的培养与引进，如加强军民融合，与地方企业合作等。

2.3 构建网络安全防范体系 为保证军队疗养院信息系统的安全稳定、高效以及可控，必须抓好顶层设计，结合云平台、网络安全态势感知新技术，制定全面的网络安全防范体系设计方案[6]。

2.3.1 优化网络规划 按照军队保密规定要求以及疗养院的业务管理，对疗养院网络按涉密程度进行划分[7]，分为与其他单位或上级沟通交流的军综网、处理内部办公或疗养业务的局域网、非涉密的互联网，严格实施物理网络隔离，一定程度上抵御了互联网上的直接威胁。对于摆渡攻击等隐患，可在军综网、局域网上使用数据加密技术、端口封锁技术，强化信息在网络上传递的保密性。另在军综网与互联网的入口配备防火墙，设置规则策略建立安全网关，对入网访问实施控制。

2.3.2 促进云平台建设 云平台是指采用多台高性能服务器通过 VMware 虚拟化技术构建计算集群，使用云计算技术将计算、网络、存储等各种软硬件技术整合，可及时掌握各服务器、存储的运行状态、警告信息等。云服务器具有天然防 ARP 攻击和 MAC 欺骗的功能，硬件冗余度高，拥有完善的监控措施，并且其动态迁移功能大大降低了故障率，保证了业务系统的连续性，因而云平台的安全性基础相较传统服务器更强。

自 2013 年起，在南京军区卫生系统利用云计算技术大力推行基于云计算的数字化医院建设工程，其目的之一意在解决医院信息化建设中安全防护方面存在的问题[8]。自全面展开实施后，云计算技术展现其优势，由于所有的数据和计算都在云端，网络不直接传递业务数据，使得数据更加安全[9]，其提供集中统一的安全防护和容灾能力，提高了医院信息系统的安全性和稳定性。目前，云平台在军队疗养院中应用尚少，我院结合自身信息化建设情况通过向医院借鉴学习，搭建了云平台系统，将疗养院局域网的大部分信息系统迁移至由 3 台高性能服务器构成的云平台上统一管理，降低了建设成本，并且在云平台上安装了杀毒软件和安全防护工具，执行严格的身份和访问管理，保证云服务器具备更高的安全性，其管理方式比传统服务器更简单高效，从根本上解决了我院信息系统管理分散、安全投入不足等问题。

2.3.3 建立网络安全态势感知预警系统 网络安全态势感知概念最早于 1999 年提出，后经一系列研究和发展，已成为提高网络安全状态认知和把控

能力的有力技术[10]。网络安全态势感知预警系统包含态势感知和监测预警两大部分，态势感知系统可对网络中的安全信息如网络设备、服务器设备、数据库、web应用等进行理解、分析并预测近期的发展趋势[11]，监测预警系统可以在网络遭到攻击前通报预警，并为管理员作安全决策提供依据。网络安全态势感知预警系统日渐在高校、政务、卫生等行业被应用，从微观至区域、宏观逐步建设，实现网络安全问题提前知晓，让网络安全防范工作更具有主动性、前瞻性[10]。如当“永恒之蓝”漏洞的变种病毒潜伏在网络中不易被发现时，医院在构建网络安全态势感知预警系统后经过对一段时间的流量采集分析，发出警告并给出详细记录，使管理员能够有针对性地实现预防，及时采取相应措施防止网络内终端被病毒攻击造成严重后果[12]。

随着智慧营区、智慧疗养概念的引入，为提高新形势下卫勤保障能力，人工智能、可穿戴智能设备等新技术被研究应用至军队疗养院保障工作中，智慧营区、智慧疗养系统的架设都需基于互联网上，这为军队疗养院系统的网络安全防范带来难度，仅依靠防火墙、防病毒等单一的安全防护手段无法满足目前的网络安全要求。军队疗养院可通过建立微观网络安全态势感知预警系统[13]，采集疗养院基于互联网的设备、系统的信息安全数据、信息威胁、风险等信息，结合互联网大数据分析的威胁情报库，对网络安全态势感知状况进行实时监控，实现疗养院网络安全问题提前判断报告、防御和响应的功能，提高疗养院网络安全的预防和响应能力，进一步加强网络安全体系建设，为疗养院卫勤信息化水平提升奠定基础[14]。

3 结　语

网络安全管理与防护是军队疗养院信息化建设中一项长期而艰巨的工作，随着人工智能等技术的快速发展，疗养院的发展也趋于电子化、智能化方向，部分疗养保障被互联网化，更多的智能设备被引入，本文提出的建立网络安全防范体系还需要不断改进，加强新技术的研究应用。总之，如何从完善管理、提升技术等多方面加强军队疗养院网络安全防护能力，将始终是军队疗养院需要探讨的一个重要课题。

[参考文献]

[1] 郑　蕾，翁盛鑫，黄　影.医院信息系统客户端的安全管理和时间[J].医疗卫生装备，2010，31(3)：62-63.

[2] Rass S.On game-theoretic network security provisioning[J].Network and Sys Manage，2013，21(1)：47-64.

[3] 潘　云.军队疗养院信息网络安全问题与管理措施[J].实用医药，2015，15(4)：197.

[4] 宋启哲，过贵元，林　琳，等.数字化疗养院建设的实践与探讨[J].东南国防医药，2013，15(6)：648.

[5] 参考国际电信联盟官方网站，https://www.itu.int/en/ITU/studygroups/com17/Pages/cybersecurity.aspx.

[6] 肖　扬，郭志旭，于海铸，等.军队互联网医院信息安全体系的构建与应用[J].中国数字医院杂志，2017，12(8)：20.

[7] 杨　俊，刘敏超.军队医院网络安全与风险控制[J].中国卫生信息管理杂志，2015，12(2)：171.

[8] 陈利佳，李刚荣，汪　鹏.服务器虚拟化技术在临床信息中心的应用探索[J].中国数字医学，2012，7(9)：65-67.

[9] 朱元元，吴国玲，徐　磊，等.“医云工程”助推数字化医院建设转型转变[J].解放军医院管理杂志，2015，22(1)：90-91.

[10] 胡建平，郝惠英，何　祺，等.卫生健康行业网络安全态势感知平台建设探讨[J].中国卫生信息管理杂志，2019，16(1)：4-8.

[11] 陈广辉.基于态势感知的安全监测预警平台研究[A]；第四届全国信息安全等级保护技术大会论文集[C].北京：全国信息安全等级保护技术大会，2015：106-110.

[12] 莫禹钧，潘愈嘉，黄　捷.医院网络安全态势感知系统构建[J].医学信息学杂志，2018，39(12)：25-28.

[13] 王丹琛，徐　扬，李　斌，等.基于业务效能的信息系统安全态势指标[J].清华大学学报(自然科学版)，2016，56(6)：517-521.

[14] 马锡坤.医院信息安全支撑体系建设的思考[J].医学研究生学报，2019，32(3)：286-289.

(收稿日期：2019-05-08；　修回日期：2019-08-27)

(责任编辑：刘玉巧)