《中国卫生质量管理》第28卷 第8期(总第165期)2021年08月

血站信息安全问题分析及应对策略*

——赵小洪 田耘博* 欧阳熊妍 何 涛

【摘 要】 从血站信息安全角度,针对物理安全、网络安全、系统安全、应用安全、数据备份与恢复等技术层面,以及安全制度、安全机构、人员安全管理、安全建设、安全运维等管理层面,分析了影响血站信息安全性的主要问题,并针对性提出应对策略,为血站信息安全管理提供参考。

【关键词】 血站;血液质量;信息安全;问题分析;应对策略

中图分类号:R197.6;R457.1+2 文献标识码:B

Analysis and Countermeasures of Information Security Problems in Blood Centers /ZHAO Xiaohong, TIAN Yunbo, OUYANG Xiongyan, et al.//Chinese Health Quality Management, 2021, 28(8): 77-79

Abstract From the perspective of information security in blood center, the main problems that affect the information security were analyzed from technology aspects of the physical security, network security, system security, application security, data backup and recovery; and from management aspect of security system, security agencies, personnel safety management, safety construction, safety operation and maintenance. Furthermore, countermeasures were put forward, which provided reference for information security management in blood center.

Key words Blood Center; Blood Quality; Information Security; Problem Analysis; Countermeasures

First-author's address Chongqing Blood Center, Chongqing, 400052, China

血站信息化水平伴随着网络技术的发展而提高,献血预约、信息录入、血液检测、发放、检测结果及献血记录查询等都已与信息进步息息相关。然而,信息安全观念淡薄,安全管理体系不健全,信息安全专业人员缺乏等情况在血站依然存在[1]。按照《中华人民共和国网络安全法》《血站质量管理规范》等文件要求,血站需对所收集、存储的数据进行保护。信息安全的实质是保护信息资源免受各类干扰、破坏和安全威胁[2-3]。现有血站信息安全文献[4-6]多从数据安全、信息系统安全、安全等级建设、病毒与攻击防护等方面进行论述。信息安全涉及诸多层面,仅从某方面做好安全防护,已不能适应日趋严峻的网络安全形势需求。本研究从血站整体信息安全角度出发,对技术和管理层面的信息安全问题进行分析并提出应对策略,旨在为血站信息安全管理提供参考。

1 问题分析

伴随血站业务开展而产生的各类信息,在其传输、存储和处理等过程中均存在信息安全风险[7],其风险可划分为技术和管理两类。

1.1 技术风险[8]

1.1.1 物理安全风险 各类计算、网络、存储等硬件设备及物理链路因断电、部件老化、不可抗力和其他因素影响不能正常使用[9],部分中小规模血站重要链路未进行冗余设计,重要设备无不间断电源等,导致血站数据安全性面临严峻挑战。

1.1.2 网络安全风险 边界防护不严格,内外网未进行隔离,安全策略配置不当,采血点与内部通信时信道未加密,对外部攻击不能准确预防和快速阻断,对内部攻击、病毒感染、恶意流量等无法迅速定位,严重影响血站内部数据传输。

DOI:10.13912/j.cnki.chqm.2021.28.8.20

*基金项目:重庆市渝中区技术预见与制度创新项目(20180163)

赵小洪 田耘博* 欧阳熊妍 何 涛 通信作者:田耘博

重庆市血液中心 重庆 400052

1.1.3　系统安全风险　使用盗版操作系统，不恰当的安全策略，无漏洞发现和补丁管理机制，使用共享、远程桌面等高危端口，滥用移动存储介质，重要系统不具备故障恢复能力，重要服务中断后不能自动恢复等，导致软件、系统等服务暂停、运行缓慢或无法使用，甚至导致采供血业务数据丢失、泄露，进而影响采供血及相关业务的正常开展。

1.1.4　应用安全风险　应用系统安全机制缺失或策略不当，部分血站以明文方式传输采供血信息，数据库或备份文件中敏感信息明文存储，日志记录粒度或保存时限不能满足《中华人民共和国网络安全法》的时限要求，未建立系统故障应急处置方案，未定期开展应急演练等，可能造成献血者信息泄露、采供血过程无法追溯、业务不能连续开展等信息安全及法律风险。

1.1.5　数据备份与恢复风险　不恰当的数据备份任务，定期核查机制缺失，备份不及时，没有数据恢复方案，恢复方案未进行定期演练，数据没有异地备份等，会造成特殊情况下备份数据不可用或恢复失败的安全风险。

1.2　管理风险

1.2.1　安全制度风险　信息安全工作没有总体方针、总体目标、范围、原则等，未通过制度对安全管理内容进行明确，未建立日常管理操作规程等，导致信息安全工作难以开展。

1.2.2　安全机构风险　未建立安全管理领导小组和安全管理工作职能部门，未配备信息安全管理人员等。

1.2.3　人员安全管理风险　工作人员信息安全意识淡薄，缺乏基本安全技能，安全意识培训未涵盖岗位相关安全知识等。

1.2.4　安全建设风险　信息系统安全建设没有总体规划，安全策略、技术架构、管理策略、建设规划等未统筹考虑。

1.2.5　安全运维风险　运维过程不可监督，系统及服务最小化安装、配置文件备份等日常运维工作缺乏详细规定，未及时与外包服务提供商签订安全协议等。

2　应对策略

没有管理，技术将沦为摆设；没有技术，管理条文也不能抵御安全威胁[10]。因此，无论是技术还是管理，信息安全隐患都应引起相关管理者的高度重视。

2.1　技术层面

2.1.1　物理安全　物理安全是计算机信息系统安全的前提。血站机房应符合GB 50174－2017《数据中心设计规范》和GB/T 22239－2019《信息安全技术网络安全等级保护基本要求》的要求，并从环境安全、设备安全和人员控制等方面提升物理安全性。可将UPS、存储、网络、计算等IT及相关设备纳入重点保护范围，有条件的可考虑设备、链路冗余和数据容灾建设等。

2.1.2　网络安全　网络是各信息设备间通信的基础，是数据传输的桥梁。血站可根据不同安全保护需求划分安全区域并设置防护策略，构建专用或加密的传输通道；从访问控制、网络隔离、VLAN划分、入侵检测与防护等方面提升技术水平，增强对威胁的预防和阻断能力；通过对网络状况、流量进行实时监测，执行严格的网络接入管控措施，精确到IP及端口级的访问控制，实现对网络威胁的及时发现、迅速定位与快速阻断，确保内部业务数据传输和采供血业务信息系统安全。

2.1.3　系统安全　操作系统是计算机系统最基础的软件，其安全职能是其他软件安全职能的根基[11]。血站可通过购置正版或国产操作系统，规避使用盗版带来的法律和安全风险。需定期对重要系统进行漏洞扫描，并根据扫描结果对现有安全措施是否完备进行研判；限制或关闭共享、远程等高危端口，业务端口按需开放，安装病毒防护软件，严格限制移动存储介质使用；重要系统定期备份并进行恢复演练，通过自动化运维等措施确保重要服务在无人值守时能够自动从中断状态恢复，避免因系统漏洞、故障引起的运行缓慢、服务暂停、数据丢失、信息泄露等问题，确保采供血及其相关业务正常开展。

2.1.4　应用安全　对物理、网络和系统进行排查与处理是为了确保应用稳定运行。血站可综合考虑如下措施：(1)新建信息项目需考虑基于Linux内核的国产系统兼容性，以顺应系统自主可控的发展趋势；(2)完善采供血相关应用的安全管理能力，并配置适宜的安全策略，严格划分用户权限、修改或清除默认账户，及时修补已知漏洞等，以提升应用程序本身的安全性；(3)通过加密协议或安全设备等确保血站多种业务场景下数据以密文形式在信道中传输，通过调整软件功能等确保敏感信息在数据库或数据库备份文件中以密文形式存储；(4)通过部署数据库审计系统提升对存取和修改数据库元素的用户进行追踪审计的能力，并对操作日志进行记录和依法留存；(5)建立涵盖应用系统多种故障的应急处置方案，并对方案进行定期演练和持续改进。

2.1.5　数据备份及恢复　有效的数据备份和备份恢复方案是信息系统安全的最后一道屏障。血站可采

取数据定期备份、任务监测、数据有效性验证、恢复方案定期演练、备份数据异地存储等措施，确保特殊情况下数据可迅速恢复。

2.2　管理层面

2.2.1　制定安全管理制度　制定包含信息安全工作的总体方针、目标、范围、原则等的安全框架，建立各类安全管理制度，逐步构建由安全策略、管理制度、操作规程等构成的信息安全管理体系。

2.2.2　建立健全安全机构　血站应设置信息安全领导机构，设立信息安全管理工作职能部门，并配备信息安全管理人员。

2.2.3　做好人员安全管理　定期组织血站工作人员进行基本安全技能培训，根据不同岗位制定不同培训方案，以确保培训内容涵盖岗位相关安全知识[12]。

2.2.4　制定安全统筹规划　指定专门部门，按相关要求对信息系统的安全建设进行总体规划并制定短期、长期工作计划。根据实际情况，对安全保障体系的总体安全策略、技术架构、管理策略、建设规划以及详细方案等进行统筹考虑。

2.2.5　做好运维管理　将设备、信息系统等的管理权限划分系统、安全和审计管理角色，形成具有角色监督、相互制约、三权分立的运维管理框架；部署运维审计系统，确保运维全过程可审计、可追踪；建立操作规程等，对日常运维工作进行细化；及时与外包服务商签订安全保密协议，确保运维安全。

3　结语

作为采供血公益性事业单位，一个区域往往只有1家血站，因此必须更加重视血站信息安全，确保采供血业务工作的持续稳定开展。从目前血站信息安全态势来看，技术层面应重点加强网络安全、系统安全、数据备份与恢复等安全防护，在管理上则需更加注重管理制度、统筹规划、运维管理等建设。通过技术和管理两种手段的融合运用，做好血站信息安全防护工作。在做好基础防护的同时，血站网络安全防护应逐步向云计算、物联网、移动互联、工业控制等新网络、新业态拓展，以确保采供血业务的全程安全防护。

网络安全不是静止的、一成不变的。做好血站网络安全工作，应根据信息安全形势对技术和管理措施进行动态调整，逐步构建起信息安全防御体系，从而为采供血事业健康发展保驾护航。

参考文献

[1]　高　瑜.采供血机构信息安全管理缺陷分析与防范策略[J].中国输血杂志，2007，20(3)：243－245.

[2]　刘城汾.网络信息安全常见问题及其对策[J].科技与企业，2015(12)：69.

[3]　范　红.信息安全风险评估实施教程[M].北京：清华大学出版社，2007：1.

[4]　李　响.血液信息管理系统中数据库信息安全的探索建设[J].电脑知识与技术，2017，13(27)：3－4.

[5]　蔡海岩.采供血机构信息安全等级保护建设方案与实践[J].信息安全，2014(11)：165－166.

[6]　韩平臣.血站网络安全面临的问题及应对措施[J].河北企业，2015(10)：42.

[7]　薛　帅.采供血机构信息安全问题及其管理[J].信息与电脑：理论版，2017(7)：210－211.

[8]　黄传河.网络规划设计师教程[M].北京：清华大学出版社，2009：424－445.

[9]　张　谦，张梦涵.血站日常信息安全实践的不足探讨[J].电脑开发与应用，2013(1)：66－68.

[10]　袁　红.采供血机构信息安全对策与研究[J].中国卫生产业，2012(27)：176.

[11]　张焕国.信息安全工程师教程[M].北京：清华大学出版社，2016：406.

[12]　李红云，李云飞，刘香云，等.如何做好血站质量管理[J].中国卫生质量管理，2013，20(2)：79－80.

通信作者：
田耘博：重庆市血液中心主任技师
E－mail：microtian@126.com

收稿日期：2020－10－30
修回日期：2021－01－04
责任编辑：吴小红

医非博不能通，非通不能精，非精不能专。必精而专，始能由博而约。

——赵晴初《存存斋医话稿序》