基于态势感知平台的大型医院网络安全风险管理实践*

孙保峰 张伟祎 杨 扬 李郁鸿

（郑州大学第一附属医院信息处 郑州 450002）

〔摘要〕 **目的/意义** 分析大型医院态势感知平台所监测到的网络安全风险事件，探明其产生的原因，提出解决方法和改善建议。**方法/过程** 以郑州大学第一附属医院为例，对态势感知平台风险事件聚合分析，筛选医院内网风险终端，并进行整改加固，分析风险终端的科室分布和成因，提出改善建议。**结果/结论** 医技科室风险终端数量较多，主要原因在于缺乏管理及未做到防病毒软件全覆盖。通过风险终端整改加固，网络安全风险事件数量明显减少。加强医院终端安全管理、提升人员网络安全意识、分区加强网络安全防护可有效降低医院网络安全风险事件发生率，提升医院网络安全防护能力。

〔关键词〕 大型医院；态势感知平台；网络安全；风险终端

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2024.10.015

Practice of Cybersecurity Risk Management in Large Hospitals Based on a Situational Awareness Platform

SUN Baofeng, ZHANG Weiyi, YANG Yang, LI Yuhong

Information Department, the First Affiliated Hospital of Zhengzhou University, Zhengzhou 450002, China

〔**Abstract**〕 **Purpose/Significance** To analyze the network security risk events monitored by the situational awareness platform of large hospitals, to find out the causes, and to put forward solutions and suggestions for improvement. **Method/Process** Taking the First Affiliated Hospital of Zhengzhou University as an example, the paper analyzes risk events on the situational awareness platform, screens the risky terminals on the hospital intranet, carries out rectification and reinforcement, analyzes the department distribution and causes of risky terminals, and puts forward suggestions for improvement. **Result/Conclusion** The number of risky terminals in medical and technical departments is large, mainly due to the lack of management and the lack of full coverage of antivirus software. Through the rectification and reinforcement of risky terminals, the number of network security risk events has been significantly reduced. Strengthening the hospital terminal security management, enhancing staff awareness of network security, and strengthening network security protection in different areas can effectively reduce the incidence of hospital network security risk events and improve the hospital network security protection capability.

〔**Keywords**〕 large hospital; situation awareness platform; network security; risky terminal

1 引言

随着“互联网＋医疗”模式与数字化医院建设的迅速推进，医院信息系统数量激增，网络规模急剧扩大，呈现出设备数量多、分布广、管理难度大

〔修回日期〕 2024－08－27

〔作者简介〕 孙保峰，工程师，发表论文9篇；通信作者：杨扬，高级工程师，硕士生导师。

〔基金项目〕 河南省医学科技攻关计划软科学重点项目（项目编号：RKX202201007）。

的特点。同时，越来越多的医疗业务暴露于互联网，医院信息开放程度加大，导致网络边界趋于模糊，医疗行业网络安全事件频发，数量呈指数级增长[1]。传统安全防护体系及其设备已无法应对日益复杂的自动化网络攻击手段[2]，越来越多的医疗机构部署了以态势感知平台为基础的主动防御系统[3-6]。本文以郑州大学第一附属医院现实网络环境为例，探讨基于态势感知平台的医院网络安全风险事件的排查、定位及处理，提出一系列旨在提升医院网络安全风险管理能力的建议，以期为其他医疗卫生机构的网络安全管理工作提供参考和借鉴。

2 资料与方法

2.1 资料

案例医院分 4 个院区，同一网络、同一系统、统一管理，2023 年 6 月上线态势感知平台，对全院 11 512 台终端、800 台服务器进行资产纳管。以 2023 年 10 月 1—31 日为统计区间，态势感知平台共检测网络安全事件数据 3 825 679 条，事件类型及攻击阶段分布，见图 1。

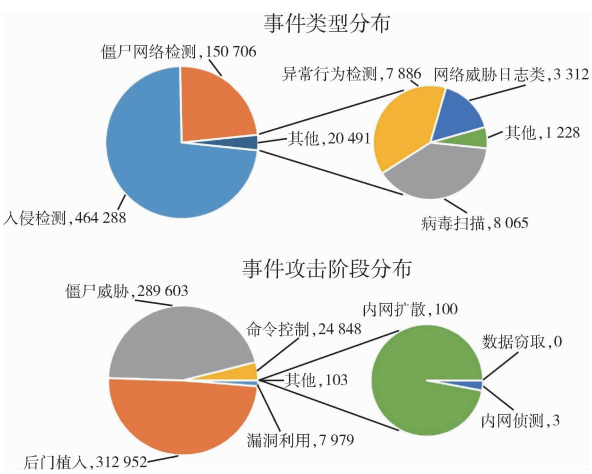

图 1 案例医院态势感知平台网络安全事件分布

2.2 方法

2.2.1 聚合分析 态势感知平台检测到的风险事件来源可分为外部互联网安全风险事件和内部网络安全风险事件[7-8]。外部互联网安全事件主要包括来自互联网的攻击试探和扫描，可将态势感知平台与边界安全防护设备联动实现外部攻击的自动阻断；内部网络安全事件主要指院内已感染终端的内网侦测和横向扩散，需要医院管理人员对风险终端进行定位、整改与加固，加强内网终端的安全管理是减少医院内部网络安全风险事件的根本途径[9-10]。对网络安全事件进行聚合分析，形成威胁事件统计表，排名第 1 位的威胁事件为 SMB Double pulsar 远程代码执行漏洞（CVE－2017－0143），共有 75 个源地址（internet protocol address，IP）对其他终端发起攻击 285 336 次，排名前 20 位的威胁事件及其攻击次数，见表 1。排除互联网公网地址对医院设备的网络攻击，对院内攻击源 IP 进行统计汇总，医院风险设备总量为 337 台，其中服务器 25 台，终端 312 台。

表 1 威胁事件攻击次数前 20 位

威胁名称	攻击次数
CVE－2017－0143	285 336
僵尸网络 IP 服务器	147 637
检测到黑客工具 RemCom	121 462
HTTP URI 长度超限	9 632
SMB 服务扫描攻击	7 886
DNS 查找 Win32/Beapycnc 域名	6 740
Trojan/IOC. APT	6 453
僵尸网络域名服务器	5 660
爬虫攻击	3 641
CVE－2017－0144	3 533
CVE－2013－4547	3 244
跨站脚本攻击	2 321
间谍代理软件活动	2 152
MSSQL 暴力破解	1 890
WannaCry DNS 查找	1 654
Trojan：Win32/remote exec	1 575
Single char EXEdirect 疑似木马下载	874
CVE－2008－3021	852
Sinkhole 响应 Kryptos Logic	834
MS17－010 漏洞扫描	831

2.2.2 风险服务器安全处置 25 台风险服务器均位于数据中心机房。其中 17 台为应用厂商未安装恶意代码防范软件，8 台为厂商运维工程师私自卸

载恶意代码防范软件，导致服务器被终端感染勒索病毒后对全网发起扫描和攻击。查明原因后，已全部安装服务器版安全防护软件并全盘查杀，消除安全隐患。

2.2.3 风险终端安全处置 案例医院终端数量多且分布广，风险终端处置过程中存在定位困难的问题，通过以下 3 种方式对风险终端进行安全处置。（1）网络定位处置。利用同一网段终端获取风险终端网卡物理地址（media access control address，MAC），在交换机上查找其所在的网络接口并关闭，强制风险终端离线。以思科交换机为例，主要操作命令为 show mac add | include XXXX. XXXX. XXXX、show cdp nei 等。（2）漏洞利用处置。利用态势感知平台获取风险终端操作系统漏洞，利用 Kali Msfconsole 工具攻击系统漏洞，获取风险终端管理权限，远程对操作系统升级加固。以内网终端普遍存在的 MS17－010 操作系统漏洞为例，主要操作命令包括 use auxiliary/scanner/smb/smb_ms17_010、use exploit/windows/smb/ms17_010_eternalblue、set rhost ip、set lhost ip 等。（3）人工排查处置。对利用上述两种处置方法仍无法定位的风险终端，由信息技术人员根据 IP 及 MAC 地址现场排查，定位风险终端并安装准入控制及杀毒软件加固处置。

2.2.4 互联网风险事件处置 针对互联网公网地址的扫描、爆破和攻击尝试，通过态势感知平台联动边界网络安全设备如防火墙、入侵防御系统（intrusion prevention system，IPS）等，设定自动处置剧本，实现对互联网风险事件的自动处置。

3 结果

3.1 基本情况

对 337 台风险终端和风险服务器整改加固后，选取 2023 年 12 月 1—31 日为统计区间，态势感知平台网络安全事件总数为 554 418 条，与前一统计区间网络安全事件数量对比，见表 2。对风险终端进行整改和加固后，全院网络安全事件数量急剧下降，医院网络安全环境得到明显提升。

表 2 态势感知平台网络安全事件数量对比

组别	整改前（条） 2023 年 10 月	整改后（条） 2023 年 12 月	下降率（%）
网络安全事件总数	3 825 679	554 418	85.5
入侵检测	464 288	168 736	63.7
僵尸网络检测	150 706	38 239	74.6
病毒扫描	8 065	980	87.8
网络威胁日志类	3 312	217	93.4

3.2 风险终端分布

全院 312 台风险终端与临床及医技科室的对应关系，见图 2，除全院公用的自助终端外，风险终端数量较多的为放疗科、手术部、磁共振（nuclear magnetic resonance imaging，MRI）室、计算机断层扫描（computed tomography，CT）室、超声科等医技科室。这些科室检查、治疗设备较多，终端品牌及型号多样，除医院信息中心运维人员外，还有大量医疗厂商运维人员，是医院网络安全防护的薄弱环节。

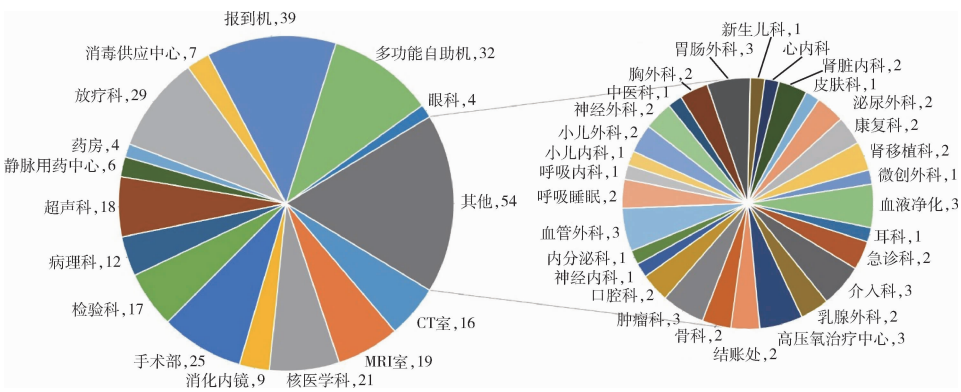

图 2 风险终端数量与临床及医技科室分布

3.3 风险终端成因分析

医院终端安全管理制度要求所有终端安装准入控制和杀毒软件后方可接入医院内网，不符合要求的终端无法访问内网应用系统。经排查，风险终端均未安装准入控制和杀毒软件，无法访问内网业务系统，但终端之间仍可相互访问，导致病毒及恶意代码横向扩散。风险终端在 CT 室、MRI 室、放疗科等临床医技科室分布较多，主要原因有以下两个方面。一是这些科室医疗设备较多，很多为医疗设备配套采购，由医疗设备运维工程师负责安装调试，医院信息管理部门参与有限。二是厂商工程师为维护方便，未遵照医院终端安全管理规定，逃避终端安全管理软件的安装。通过现场访谈，风险终端的成因主要有 4 个，风险终端成因与对应数量，见表3。

表3 风险终端成因及分布

成因	数量（台）	比例（%）
缺乏管理，不关注是否安装	124	39.70
医疗设备厂商不建议安装	83	26.60
已安装免费版杀毒软件	60	19.20
不了解终端安全管理制度，未安装	45	14.40

4 讨论

4.1 医院网络安全管理现状

重信息系统防护，轻终端安全，重网络出口安全，轻内网管理，是当前医院信息安全保障工作的典型问题[11-12]。为满足网络安全等级保护制度的要求，医疗机构均建立终端准入管理制度，但仍存在部分终端未安装准入管理客户端而接入医院内网的情况。这部分终端主要分布在医技科室，大多由设备管理科购置医疗设备时伴随入院，接入医院内网时未履行严格的安全检查，医技工作人员缺乏网络安全意识，疏于安全管理[13]。

4.2 提升医院网络安全风险管理能力的建议

4.2.1 科学分区，构建综合防御体系 对医院网络结构科学分区，如按照不同功能将网络分为互联网区、隔离区域、内网接入区和内网核心服务器区。（1）互联网区。互联网区主要提供对外应用发布、负载均衡、用户上网等服务，是最容易被攻击的区域，可通过设置白名单、减少对外开放端口、缩小攻击面、部署入侵防御系统等措施增强网络防护。（2）隔离区域。隔离区域通常部署对外提供服务的服务器，既需要对外提供服务，又需要连接医院内网获取数据，容易成为黑客攻击的跳板，可通过部署微隔离、双向网闸、基于主机的入侵检测系统增强网络防护。（3）内网接入区。内网接入区主要提供内网终端的接入，包括便携式笔记本、自助终端、监控设备、物联网终端等，可根据终端类型设置不同的准入管理策略、安装杀毒软件、采用零信任技术等增强网络防护。如在风险终端分布较多的医技科室，采用防勒索交换机作为接入设备。（4）内网核心服务器区。内网核心服务器区为医院核心信息系统运行区域，也是要保护的核心区域，可通过安全分级设置不同的隔离和管控措施、安装防御软件、权限最小化管理等措施增强网络防护。如部署终端检测响应系统。

4.2.2 制定终端安全管理制度，狠抓落实 由于风险终端的最主要成因是终端未安装防病毒软件、未履行终端准入管理，为提升医院网络安全防护能力、保障医疗数据安全，应根据医院实际制定终端安全管理制度，具体包含终端采购、终端准入、终端巡检等制度。终端采购制度应明确医院信息部门全流程参与终端尤其是医疗终端的采购管理。终端准入制度应明确终端接入医院内网的前提条件，不符合安全基线要求的终端不得接入内网。终端巡检制度应要求医院信息部门、使用部门定期对接入内网的终端进行安全巡检，排查终端准入控制软件、防病毒软件安装及病毒库升级情况，定期对终端漏洞进行整改和加固。

4.2.3 建立预警与响应机制，定期演练 基于态势感知平台对网络流量实时检测与分析，设定明确的网络异常指标，如流量异常、登录失败次数超限、恶意软件活动等，建立自动化的网络安全事件预警系统，一旦检测到安全威胁，系统自动发送警

报[14]。安全管理人员根据安全事件威胁等级，制定详细的响应流程，包括事件识别、评估、隔离、通知、修复、验证等步骤。事后对每次响应事件进行综合评估，持续改进预警和响应机制。定期开展网络安全应急演练，检测预警与响应机制的合理性、可操作性，提升安全团队应急响应能力。

4.2.4 加强安全意识培训，打造“人肉防火墙”

定期对医院全体工作人员进行网络安全意识培训，使其了解网络安全的基本知识、掌握常见网络安全威胁和攻击方法，学会正确的网络安全防护和应急措施。消除因使用人员不清楚而出现的风险终端。全员参与，使员工在头脑中筑起网络安全的“防火墙”。

5 结语

态势感知平台通过对网络流量实时分析和处理，产生大量网络安全事件和告警，如何对风险事件和告警排查、分析及处理，成为医疗机构网络安全管理人员的工作痛点[15]。本文以郑州大学第一附属医院生产环境为例，阐述基于态势感知平台的网络安全风险事件处置过程。由于大型医院终端设备数量多、分布广，风险终端定位难，综合利用网络定位、漏洞利用和现场人工排查的方式对风险终端安全加固。通过对风险服务器及风险终端的安全加固，极大提升了医院网络安全防护能力，降低了医院网络安全风险事件数量。基于医疗机构网络安全管理现状，提出提升医院网络安全风险管理能力的建议。态势感知平台检测网络威胁的能力与流量采集探针的数量及安装位置密切相关，仅依靠此平台无法检出全部网络威胁[16]，如虚拟化集群内部的网络威胁等，下一步将继续完善网络安全防御机制，持续增强医院网络安全防护能力。

作者贡献：孙保峰负责方案实施、论文撰写；张伟祎负责资料整理、论文修订；杨扬负责方案论证；李郁鸿负责方案设计。

利益声明：所有作者均声明不存在利益冲突。

参考文献

1 莫禹钧，黄捷，潘愈嘉. 基于网络安全态势感知的主动防御系统设计与实现［J］. 医学信息学杂志，2020，41（3）：60－63.

2 徐晨，常晓磊，吴振洲，等. 基于零信任安全的云网管理平台应用透析［J］. 网络空间安全，2024，15（1）：85－90.

3 袁骏毅，潘常青，宓林晖. 基于等级保护 2.0 标准体系的医院信息化安全建设与研究［J］. 中国医院，2021，25（1）：72－73.

4 李泽慧，徐沛东，邬阳，等. 基于大数据的网络安全态势感知平台应用研究［J］. 计算机应用与软件，2023，40（7）：337－341.

5 侯爽，李寅，杜元太. 医院态势感知网络安全平台建设实践［J］. 中国卫生信息管理杂志，2023，20（5）：808－813.

6 陈明，林志刚，林传捷. 基于态势感知的医院安全运营实践［J］. 中国卫生产业，2022，19（10）：98－101.

7 舒婷，赵韡，徐帆，等. 患者安全目标：智慧医院建设中的网络安全风险［J］. 中国卫生质量管理，2020，27（6）：24－27.

8 潘愈嘉，陆丹艳. 以网络态势感知平台为核心的医院局域网安全运维实践［J］. 中国数字医学，2020，15（12）：10－13.

9 刘海一. 医疗设备维护管理与医院网络安全探讨［J］. 中国数字医学，2023，18（9）：9－12.

10 邱皓文，陈东东. 浅谈医院内网终端安全问题及应对［J］. 信息技术时代，2023（7）：41－43.

11 孟晓阳，孙国强，林泽奇. 医院计算机终端安全防护研究与实践［J］. 中国卫生信息管理杂志，2019，16（1）：13－17.

12 李智一，肖勇，沈绍武. 湖北省中医医院网络安全建设现状分析与思考［J］. 医学信息学杂志，2024，45（4）：91－96，102.

13 陆婷娟，肖征，晏亚，等. 医院网络安全实行终端准入管理的探析［J］. 中国数字医学，2021，16（2）：113－116.

14 姚涵，孟晓阳，卢涛，等. 智能化技术趋势下医院信息化建设研究［J］. 中国医院管理，2023，43（12）：60－63.

15 刘孝鼎. 医院网络安全防御管理系统透析［J］. 网络空间安全，2024，15（2）：78－81.

16 吴山君. 态势感知平台在医院信息安全管理中的应用分析［J］. 中国信息界，2024（2）：22－24.