基于安全感知平台的医院信息安全等级保护整改方案设计

黄 捷 潘愈嘉 莫禹钧

（贵港市人民医院 贵港 537100）

〔摘要〕 依照信息系统网络安全等级保护 2.0 的最新要求，结合医院信息安全建设现状，设计基于安全感知平台的医院信息安全等级保护整改方案，详细阐述方案目标、总体设计、具体内容，指出该方案实施为医院信息化建设安全提供重要保障。

〔关键词〕 安全感知平台；等保 2.0；网络安全；整改方案

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2020.02.014

Design of Rectification Plan for Hospital Information Security Level Protection Based on Security Awareness Platform *HUANG Jie, PAN Yujia, MO Yujun, People's Hospital of Guigang, Guigang 537100, China*

〔**Abstract**〕 In accordance with the latest requirements of information system network security level protection 2.0, together with the current situation of hospital information security building, the rectification plan for hospital information security level protection based on security awareness platform has been designed. The paper elaborates on the plan goals, overall design, and specific contents, points out that the implementation of this plan provides an important guarantee for the safety of hospital informatization building.

〔**Keywords**〕 security awareness platform; security level protection 2.0; network security; rectification plan

1 引言

近年来信息技术日新月异，医院信息化伴随着“互联网＋医疗”时代的来临快速发展，然而诸如 WannaCry、GandCrab 等勒索病毒的出现严重威胁医院信息安全。贵港市人民医院是一家大型三级甲等综合性医院，该院信息系统建设经过 10 多年的不断深化，目前已覆盖各个部门，同时涵盖患者就诊各个环节。由于医院信息系统涉及大量私密信息如财务数据、药品耗材、就诊信息、电子病历等，一旦出现医疗信息泄露和传播的严重问题将会对医院和患者造成难以弥补的损失。

为有效管控频发的医疗信息泄密事件，国家先后制定一系列法律法规来保障医疗信息安全，其中信息安全分级保护制度的主要目的就是保护系统安全，保证敏感信息的处理、提高信息系统防护能力和应急水平。2019 年《信息安全技术 网络安全等级保护基本要求》新国标正式发布，标志着网络安全等级保护已进入 2.0（以下简称等保 2.0）时代，同时也意味着医院信息安全等级保护整改势在必行。以等级保护 3 级系统为例，新的防护标准要求分类，见图 1。

〔收稿日期〕 2019－06－13

〔作者简介〕 黄捷，中级工程师，发表论文 3 篇；通讯作者：潘愈嘉，高级工程师。

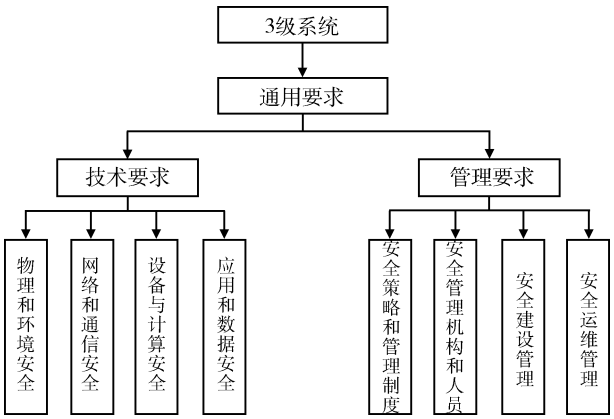

图1 等保2.0 3 级系统防护要求分类

2 信息安全建设现状及系统设计目标

2.1 现状分析

2011 年原卫生部印发《卫生行业信息安全等级保护工作的指导意见》通知，根据文件精神贵港市人民医院一直关注信息安全，坚持以 3 级安全等级保护要求作为信息化建设的规范和标准[1]。2017 年医院核心业务信息系统包括医院信息、检验信息、医学影像存储与传输系统及电子病历已顺利通过信息安全等级保护 3 级测评，但随着等保 2.0 新国标的出现并结合日常工作实际情况，医院信息安全等级保护体系在网络和通信、设备和计算安全方面存在着以下问题：为通过合规性检查，添加各种安全设备，割裂的防护措施无法直观呈现安全状态，还给运维带来巨大负担。安全设备上配置静态防御策略，对资产变化、攻击行为不能持续检测，缺乏动态监测威胁的能力。本地防护措施能阻断大部分攻击，但对于紧急事件应变处置能力较差，一旦发生安全事件容易导致资产、形象受损。医院数据中心采用虚拟化技术，安全边界模糊，物理设备无法直接分区分域防护，无法应对平台和虚拟机之间的威胁。

2.2 设计目标

针对上述问题，本研究在充分考虑等保 2.0 新国标关于网络和通信、设备和计算安全两个重要方面的基础上，设计基于安全感知平台的医院信息安全等级保护整改方案，部署针对全网流量进行检测、预警、响应处置的大数据安全平台，不仅可以快速发现并定位医院网络的潜在威胁，还能够以可视化的方式看清资产、看见威胁、看懂风险，从而提高医院信息安全管理效率，实现全网安全可视。

3 等级保护整改方案设计

3.1 总体设计

本方案根据《信息安全技术 网络安全等级保护基本要求（GB/T 22239 – 2008）》安全等级保护 3 级标准要求，在原有网络体系结构中进行整改，部署安全感知平台组件，构建安全运维中心，主要包括潜伏威胁探针（Security Theraten Acupuncture，STA）、应用层防火墙（Next Generation Application Firewall，NGAF）、安全感知系统（Security Information System，SIS）及其他安全组件。整改后的网络拓扑结构，见图 2。医院信息系统数据的特殊性、多样性和复杂性，以及对数据处理的准确性、安全性和实时性有着很高的要求[2]，因此本研究通过防御设备、检测设备、流量探针、威胁情报等工具向安全感知系统提供有效的数据来源，通过全流量检测和大数据自动分析处理和深度挖掘对整体网络安全态势、业务安全风险和业务访问关系等关键内容进行分析评价，感知异常行为和定位威胁，为医院信息管理人员提供可视化的网络趋势和业务决策，最后各组件之间协同工作，联动封堵和查杀木马和蠕虫病毒。

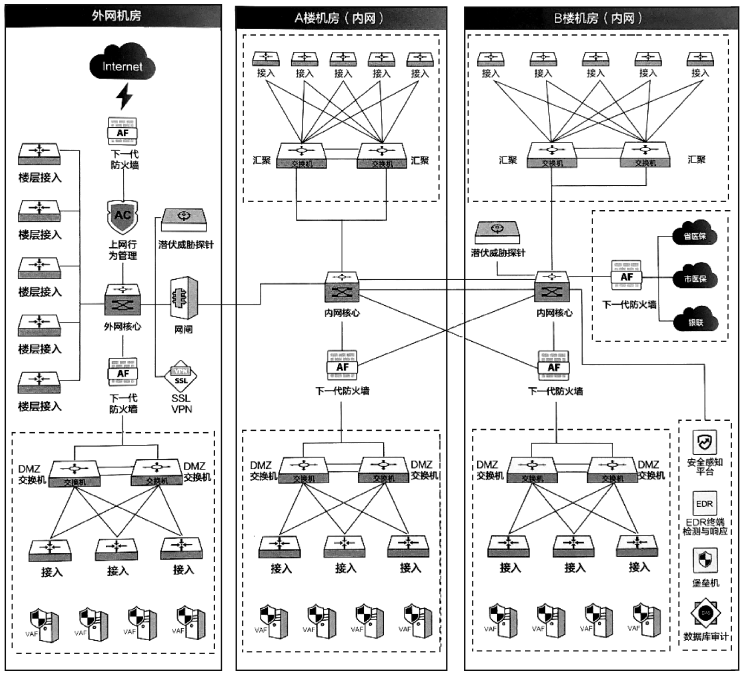

图2 整改后网络拓扑结构

3.2 安全感知平台部署方案

3.2.1 *潜伏威胁探针* 由于等保2.0在网络和通信安全入侵检测方面明确新增评分b项：“应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为”，而安全威胁往往隐藏于医院信息系统内部的网络数据中，只有全面、精准地采集网络数据才能保证后台安全数据评估系统对网络安全态势的准确预测。针对此评分项采用具有持续收集海量、多维数据功能的潜伏威胁探针设备，以旁挂方式分别部署在内网与外网核心交换机上。配置核心交换机上的流量镜像目端口，使所有连接核心交换机的网络设备产生镜像流量指向镜像目端口，结合潜伏威胁探针设备中的流量传感器从而获得医院网络链路中数据的复制信息。在持续不断地检测、监听网络数据流的过程中，探针设备通过Syslog、Netflow、SNMP等传感技术自动识别用户或服务器的网络攻击行为和业务违规访问关系，初步检测大量的多源异构数据后，提取有效数据上报至安全感知系统，其中包括原始流量、终端行为、监测数据、日志数据、异常会话、敏感数据等各种信息。在网络关键节点增加潜伏威胁探针的作用是对绕过边界防御进入内网中的攻击行为进行检测，弥补安全设备上配置静态防御策略的不足；通过对内部用户、业务资产异常行为的持续基础检测达到第一时间发现潜在风险以降低损失的目的[3]。

3.2.2 *应用层防火墙* 由于传统网络防火墙是基于网络层的传输控制协议（Transmission Control Protocol，TCP）和IP地址的状态检测来设置与加强状态访问控制列表，而近年来出现的应用层攻击诸如结构化查询语言（Structured Query Language，SQL）注入、跨站脚本攻击（Cascading Style Sheets，CSS）、恶意爬虫攻击、僵尸网络病毒、信息泄露等，传统防火墙已无法通过包头检测（Packet Headers）发现攻击与清除潜在威胁。虽然增加传统应用层设备如入侵检测系统（Intrusion Detection System，IDS）与入侵防御系统（Intrusion Prevention System，IPS）可以弥补网络防火墙的不足，但由于医院信息系统网络拓扑结构的多样性、复杂性，内外网在数据业务上存在分布式多出口、多区域的特点[4]，为做好边界防护添加多台安全设备，割裂的防护状态除增加运维负担外也极不符合等保2.0集中管控的要求。针对上述问题，整改方案中使用具有2~7层防护功能的应用层防火墙代替传统边界防护设备。应用层防火墙高度集成传统网络防火墙与入侵防御、入侵检测系统的防护功能，除向医院

信息网络提供全面的应用安全防护和访问控制功能外，还利用自身高效的应用层处理能力构建智能医院信息网络安全体系[5]。首先，在医院外网路由器出口与互联网之间部署 1 台应用层防火墙，通过基于应用的双向深度检测和流引擎查毒等技术，有效防止蠕虫、木马、缓冲区溢出攻击、口令暴力破解、黑客后门链接及 DOS/DDOS 攻击等各类已知和未知攻击。其次，在医院内网核心交换机与市医保、银联和卫健委专线等业务专线之间部署应用层防火墙，利用面向用户与应用的访问控制策略智能识别用户与内网应用，防止黑客通过专网进入医院内网，最大限度保障医院内部业务系统的数据安全。最后，在核心业务域（3 级系统域）与核心交换网络间部署应用层防火墙，利用应用协议内容隐藏、敏感信息防泄露与网页防篡改等技术有效防止系统敏感信息泄露和 Web 漏洞攻击。

3.2.3 安全感知系统 由于等保 2.0 关于网络和通信安全的集中管控原则新增以下条目：一是划分出特定的管理区域，对分布在网络中的设备或组件进行管控；二是对分散在各个设备上的审计数据进行收集汇总和集中分析；三是对网络中发生的各类安全事件进行识别、报警和分析。因此整改方案将安全感知系统以旁挂方式与内网核心交换机连接，通过添加其他安全组件集中构建安全运维中心。安全感知系统是安全感知平台的核心组成部分，首先通过海量收集汇总潜伏威胁探针、应用层防火墙等各类安全组件日志和原始流量，对采集的数据进行规格化、统一化预处理，然后利用人机共智、大数据关联等技术结合流量特征、行为分析建模，有效地对预处理的安全数据进行分析挖掘，最后通过神经网络预测技术实现网络安全趋势预测和全网业务资产的有效管控，基于可视化展示技术向医院信息管理人员清晰展示业务关系和潜在的异常访问风险。安全感知系统的可视化呈现为医院信息管理者决策提供有力依据，展示内容主要分为两个方面：一是全局可视辅助决策，通过实时监控外部攻击次数、来源、目标、类型及最新安全事件、风险应用等信息并进行整体评价，使管理人员有效掌握全网外部攻击态势，准确分析与决策；二是微观可视辅助决策，针对具体遭受病毒攻击的失陷资产以攻击链形式对资产被攻击程序进行举证，通过对失陷资产遭受攻击事件的详细分析将失陷程度和异常活动进行汇总整理为安全事件并预警提醒，以便于管理人员更清晰、直观地了解网络攻击过程和阶段，最后针对安全事件危害向管理人员提供准确的处置建议。

3.2.4 其他安全组件 （1）威胁情报系统。部署于第 3 方服务平台的安全云并通过互联网与安全感知系统对接，通过互联网大数据分析与人工智能自我学习技术实时发送最新情报数据至安全感知系统，从而提高安全威胁识别效率和准确率。（2）端点安全工具。以插件形式部署在硬件或虚拟化服务器操作系统上，不仅可以采集服务器安全数据上报安全感知系统，而且能够对木马、蠕虫病毒进行扫描和查杀。（3）上网行为管理控制器。以干路形式部署于外网核心交换机与应用层防火墙之间，一方面实现用户上网行为管理，另一方面与安全感知系统协同工作，实现用户身份的识别。（4）虚拟安全组件。虚拟机防火墙（Virtual Application Firewall，VAF）部署于各核心业务区域下的虚拟机服务器平台，通过设置严格的虚拟区域访问控制策略来防止非授权接入，从而实现对同区域、同网段的风险检测，不同区域之间业务互访首先由 VAF 进行安全控制和清洗，避免安全风险的进一步扩散。

4 结语

本研究按照网络安全等级保护 3 级规范 2.0 新国标要求，结合当前医院信息安全建设实际情况，制定基于安全感知平台的医院信息安全等级保护整改方案。通过合理构建高效、可靠的安全感平台使医院信息安全由被动防御转向主动化、动态化防御，提高网络整体安全防护能力，从而为信息化高速发展及业务安全有效运营提供有力保障。

参考文献

1 庞延辉，罗俊，肖鹏. 疾控中心信息安全等级保护整改方案设计［J］. 医学信息学杂志，2018，39（8）：44－46.

2 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）：25－27.

3 王俊. 基于等级保护的医院网络区域边界安全研究［J］. 中国数字医学，2013，8（3）：96－98.

4 王磊，魏晓艳，郎爽. 医院信息安全等级保护三级评测的应用与实践［J］. 中国数字医学，2015，10（2）：81－83.

5 陈伟，王强，袁天祥. 医疗云计算技术与信息安全等级保护［J］. 中国数字医学，2014，9（8）：26－28，31.