

“互联网 + 医疗”模式下信息安全零信任架构建设与应用

刘恒宇

(南宁市第一人民医院 南宁 530022)

〔摘要〕 分析“互联网 + 医疗”模式下网络安全问题, 提出应用信息零信任架构防护建议, 对零信任架构建设、实施路径进行阐述, 包括设置设备间访问控制与权限、实施动态网络监测等方面。

〔关键词〕 “互联网 + 医疗”; 零信任; 信息安全

〔中图分类号〕 R-056 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2020.08.011

Building and Application of Information Security Zero Trust Architecture under the Mode of "Internet + Medical" LIU Hengyu, The First People's Hospital of Nanning, Nanning 530022, China

〔Abstract〕 The paper analyzes the network security issues under the mode of "Internet + medical", makes recommendations to apply information zero trust architecture protection. It also expounds the building and implementation path of zero trust architecture, including setting up access control and authority between devices, implementing dynamic network monitoring and so on.

〔Keywords〕 "Internet + medical"; zero trust; information security

1 引言

2015 年国务院发布《关于积极推进“互联网 +”行动的指导意见》, 提出要将互联网创新成果与经济社会各领域深度融合, 包括健康医疗行业。随着“互联网 +”模式在医疗领域快速发展, 医疗数据及患者信息泄露、黑客攻击医院信息系统事件时有发生, 对患者、医院造成不良影响及经济损失。传统基于逻辑边界的防护体系主要采用内外网物理隔离, 但随着互联网医院兴起, 预约、支付、病情咨询、查阅报告向线上模式发展, 内网数据需传送到互联网, 内网服务器直接与互联网关联, 传

统防护模式失效, 可能导致内网感染木马病毒、服务器被不法分子操控等网络安全问题。在此背景下出现的零信任架构可重新构建基于身份和访问控制的逻辑边界^[1]。“零信任架构”的核心理念是在局域网内部的人员、网络设备、服务器、软件系统互相不可信, 对待安全问题不能划定一个区域后再进行防护, 容易造成特定区域内某个安全防护级别不够, 最后导致整个安全体系崩溃。传统基于逻辑边界的防护体系大多采用划分区域的规划模式, 大致分为内部服务器区、内部客户端区、隔离区 (Demilitarized Zone, DMZ)、外部客户端区, 见图 1。“互联网 +”进入到医疗行业后, 处于内部服务器区的信息需要和外部客户端进行交互, 且交互程度随互联网发展越来越深, 内部网络开放程度也越来越大, 传统逻辑边界逐渐模糊。

〔修回日期〕 2020-03-01

〔作者简介〕 刘恒宇, 助理工程师, 发表论文 1 篇。

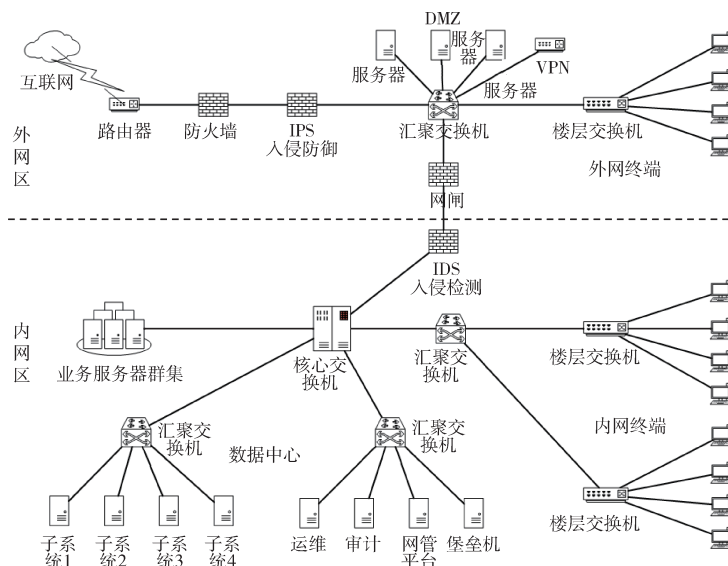


图 1 传统基于逻辑边界的防护体系

2 “互联网 + 医疗” 安全问题分析

2.1 互联网网页防护缺失

2.1.1 概述 “互联网 + 医疗” 模式必须具有面向互联网的网页，如果网页平台搭建未经网络安全公司专业检测，网络安全性达不到要求，则易受黑客等不法分子攻击。黑客等通过攻击可获取网站最高权限甚至控制整台网页服务器，造成较大安全问题。

2.1.2 存在问题 “互联网 + 医疗” 向基层医院普及，部分医院网站属于“裸奔”状态，从互联网到内网设备之间无安全设备架设，甚至网页后台和 WEB 服务器的基本安全设置不符合信息安全等级保护要求，存在问题包括：后台管理密码复杂度低、服务器直接连接互联网、互联网协议（Internet Protocol, IP）地址暴露高危端口、操作系统不打安全补丁、网页后台代码设计不考虑安全问题、网页存在注入漏洞、后台数据库未进行备份等。

2.1.3 应对措施 黑客攻击主要目的为窃取数据信息。各类医疗数据关乎民生，目前医疗数据上报国家卫健委、各级卫生单位间数据互联互通、各行业间大数据对接都需经过互联网平台，应使用数据加密、脱敏技术等手段防止不法分子从中监听或者违规收集信息。

2.2 管理端口被暴力破解

近年来“勒索病毒”横扫全球，黑客利用其攻破服务器强行加密数据库和核心文件后勒索钱财^[2]。木马病毒利用服务器漏洞进行端口扫描，入侵不经防护直接接入互联网的服务器。医疗机构如有前置机暴露在公网，则内网终端可能会感染木马病毒被黑客远程控制。“互联网 + 医疗”业务上线初期，网站实施人员为了方便远程维护基本都会要求暴露管理端口在互联网上，无形中为黑客打开“后门”。黑客通过暴力破解直接可获得服务器最高权限，控制整台服务器。前置机被攻破之后黑客可能对内网进行二次扫描，对同区域内其他服务器群进行攻击从而攻破更多服务器，造成极其严重的安全问题。

2.3 内网安全防护不到位

传统基于边界的网络安全架构认为内网是安全的，通过防火墙、Web 应用防护系统（Web Application Firewall, WAF），入侵防御系统（Intrusion Prevention System, IPS）等边界安全产品网络出口进行重重防护而忽略内网安全。前文所述两种攻破方式都是在安全边界之外的进攻。随着网络安全日益受到重视、Web 防护和安全管理日益健全，

由从外部进入的可能性降低,但内网安全隐患凸显。医疗行业业务系统较多,除医院信息管理系统、检验信息管理系统、影像管理系统等类核心业务系统外,会在内部环境搭建子系统或辅助系统。如果系统运营商服务水平不达标、实施人员身份权限管理不恰当将会导致各系统安全系数下降,一旦子系统服务器被木马程序攻击,黑客能远程在内网持续扫描其他服务器漏洞^[3]并避过所有安全设备防护,将造成极大的内网安全威胁。

3 应用零信任架构应对安全问题

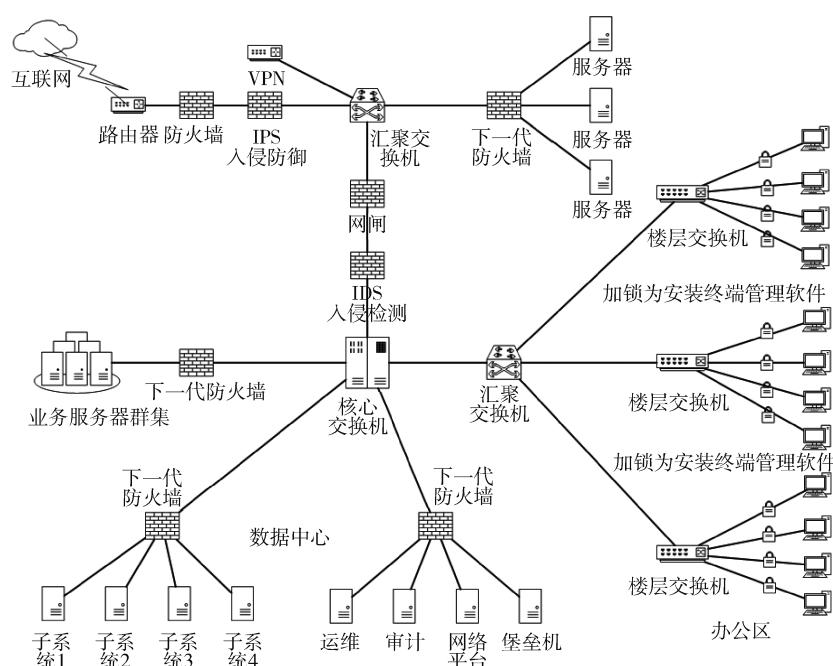


图2 零信任架构

3.2 设备间访问控制与权限

3.2.1 概述 医疗子系统和医疗设备间需要建立紧密的互联互通,且医疗行业面向患者开放,不是完全封闭的内部系统,需要进行大量数据交互以支持系统正常运作。其中互联互通安全问题较重要。对此零信任架构可起到较好防护作用。

3.2.2 防护方法 在某个医疗子系统和医疗设备间建立互不信任机制,对用户身份进行认证。如条件允许可使用多因子身份验证确保用户身份真实

3.1 基本原则及架构

零信任架构核心观点是“假定内部用户并不比外部用户可信”,包括4项基本原则:验证用户、验证设备、限制访问与权限、自适应^[4]。零信任架构安全模型为身份认证提供了逻辑清晰的管理策略。重点在保护内部网络、设备、数据和各类基础设施的信息安全。零信任架构并不是单纯隔离,可应用在不同逻辑分层下,需隔离认证环境均可采用,见图2。

性。同时认证设备,对医院公共主机、笔记本电脑、移动设备均需制定基于设备身份的访问控制策略,以最小化权限设置,只允许授信终端访问内部网络^[5]。针对对外公共主机应限定访问时间段,避免在安全人员人手不足的时间段发生网络攻击。

3.2.3 实施方案和过程 (1) 拆解传统的内外网隔离方式。不再按各类区域进行划分,每个终端独立按照统一模板进行安全基线核查,针对客户端采用终端准入系统,符合安全基线的终端才能连入网络,控制非法终端连入。(2) 服务器之间互联采

用最小化原则配置。启用默认拒绝的防火墙策略,仅允许管理员授权的端口及 IP 地址进行互联,任何未授权数据包应在网络层面默认拒绝,禁用服务器之间不必要的互联,降低木马病毒横向扩展的可能性。(3) 尽量采用不同厂家的防火墙设备。在同一数据链路上采用两种厂家的安全设备,防止同一区域内使用同一安全厂家产品可能存在相同漏洞的情况出现,避免黑客或病毒轻易穿透防护直接攻击到服务器。(4) 网络地址转换方式。医疗信息出口较其他企事业单位多,且与医保、卫健委、药品物流、银行等部门连通,因此防火墙出口应尽量使用网络地址转换 (Network Address Translation, NAT) 方式进行互联,以隐藏内部网络的路由拓扑,控制外部对院内网络的访问。(5) 网络传输数据加密。互联网前置机搭建 WebServer 时所采用网页应采用加密的超文本传输安全协议 (Hyper Text Transfer Protocol over Secure Socket Layer, HTTPS) 方式进行搭建,对网络传输数据加密,以有效防止数据被监听获取,保证数据隐私安全。(6) 运维人员应使用

虚拟专用网络 (Virtual Private Network, VPN) 连接内网。每名运维人员应该拥有不同账号,权限控制其仅能维护的服务器,VPN 采用多因子认证技术登录,如手机短信 + 账号密码的方式识别运维人员身份。(7) 内部服务器终端远程账户管理应使用堡垒机。服务器原始账号密码原则上不告知外部公司运维人员,应由堡垒机统一管理并分配运维人员账号,同时开启操作审计,禁止高危操作或越权操作。

3.3 动态监测网络中可能存在的威胁

3.3.1 防护方法 随着信息化程度逐渐提高,各种设备都部署到网络中,网络环境更加复杂,需要将“便衣警察”式的监控探针安插在关键链路及内部网络、外部网络、DMZ 网络、安全审计网络等不同环境中,以及时发现违规操作。黑客或木马病毒需要经长期嗅探、尝试、爆破才能成功入侵系统或者网络,因此在原有网络架构中架设探针服务器可进行网络实时监控,对网络高危嗅探动作进行预警,提示网络安全人员进行人为干预,见图 3。

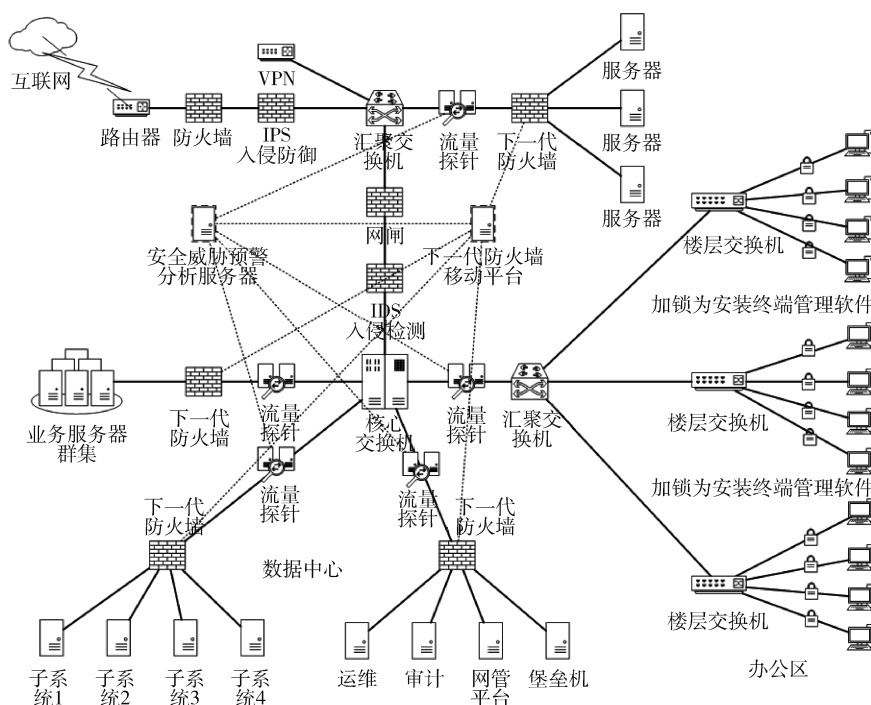


图 3 架设探针服务器进行网络实时监控

3.3.2 主要实施方案和过程 (1) 在核心交换机或下一代防火墙上建立网络镜像口。该条链路为

数据必经之路,从中能够获取直观流量信息,全网收集流量数据后对常规应用服务流量进行标记并存

入探针流量数据服务器。(2) 安装威胁预警分析服务器。分析探针流量数据并汇总已标记的应用数据,通过互联网大数据平台特征库进行数据匹配,从而分析流量是否符合恶意攻击进而进行记录和报警。(3) 部署下一代防火墙联动平台。主动控制其安全策略,接收来自安全威胁分析服务器的报警,按照管理人员预先配置的处置流程下发安全策略,实现探针和防火墙的实时联动,进行主动防御。(4) 流量探针。不仅可标记网络攻击流量,还能标记数据库、网页浏览及应用协议流量,经预警分析服务器收集由人工进行二次分析,可为运维人员进行应用层面预警,应及时修改应用代码防止漏洞被利用。随着安全设备发展,部分产品已应用人工智能技术进行防护,利用人工智能的学习能力自动对安全设备下发策略,自动阻断攻击源,配合人工配置,能够高精度识别正常和非法行为,在保证正常业务不中断的情况下阻断网络中的非法行为。

4 结语

互联网技术飞速发展,安全防护有待进一步加

强。使用零信任网络安全架构,使原本封闭环境内的资源得以安全共享并及时发现高危漏洞,提高防控程度,避免原本安全区域内某个节点被攻破后整个区域都陷入风险状态的情况。“互联网+医疗”模式在提高医疗信息化水平的同时,为患者提供方便快捷的医疗服务,但应重视信息安全,需要一套成熟且能够应对未来“互联网+”趋势下逐渐进化的架构。零信任架构将成为未来网络安全流行架构之一,网络安全将进入全新时代。

参考文献

- 1 方山,李华. 计算机网络边界安全防护管理方法研究[J]. 信息通信, 2017 (11): 155-157.
- 2 李放,韩亚坤,李曙光. 针对勒索病毒的医院安全防护体系设计[J]. 中国数字医学, 2019, 14 (11): 85-87.
- 3 廖莹璐,杭菲璐,谢林江. 浅谈企业网络终端安全与 APT 防御[J]. 自动化应用, 2018 (5): 75-77.
- 4 焦汀. 为什么说“零信任”将成为网络安全流行框架之一[J]. 计算机与网络, 2018, 44 (4): 54-55.
- 5 林辉玉,赵长林. 零信任安全呼唤新思维和新举措[J]. 网络安全和信息化, 2019 (2): 102-103.

(上接第 51 页)

4 结语

健康医疗大数据已纳入国家大数据战略布局,加快健康医疗大数据中心建设能够促进医疗服务发展和医疗资源合理流动,不断满足人民群众多层次、多样化健康需求。加强政策支持,继续汇聚更多医疗机构数据,加快大数据科研和科研成果转化,培育健康经济新动能是健康医疗大数据中心发展方向。

参考文献

- 1 国务院办公厅. 关于促进和规范健康医疗大数据应用发

- 展的指导意见(国办发〔2016〕47号) [EB/OL]. [2016-06-24]. http://www.gov.cn/zhengce/content/2016-06/24/content_5085091.htm.
- 2 赵飞,武琼,曾良怀,等. 健康医疗大数据共享开放模式研究[J]. 中国卫生信息管理杂志, 2019, 16 (6): 649-654.
 - 3 许培海,黄匡时. 我国健康医疗大数据的现状、问题及对策[J]. 中国数字医学, 2017, 12 (5): 24-26.
 - 4 国务院办公厅. “十三五”深化医药卫生体制改革规划(国办发〔2016〕78号) [EB/OL]. [2017-01-09]. http://www.gov.cn/zhengce/content/2017-01/09/content_5158053.htm.