广州医科大学附属第二医院
THE SECOND AFFILIATED HOSPITAL OF GUANGZHOU MEDICAL UNIVERSITY

医院信息安全建设实践分享

广州医科大学第二附属医院
陆慧菁

目录


VIRUS
CRACKER
INTRUDER
SPYWARE
PASSWORD
IDENTITY
CODE
UNSAFE
THEFT
HACKER

01

医院概况

医院概况

番禺院区

器官移植中心、心脑血管疾病防控中心、创伤救治中心和肿瘤防治中心

昌岗院区

高水平的急危重症和疑难复杂疾病诊治区域医疗中心

西院区

全国高水平卫生服务中心和全科医学培训示范性基地

信息化概况

构建患者服务平台，提高服务质量
- 互联网医疗
- 自助服务
- 随访服务
- 掌上医疗

打造临床信息系统，提高医疗水平
- 院前急救
- 电子病历
- 无纸化病案
- 专科病历
- 移动医疗

建立服务保障体系，保证服务质量
- 处方自动识别
- 手术分级管理
- 消毒全追溯
- 输血全流程管理

加强信息监管，保证数据及系统安全
- 三级等保
- 上网行为管理
- 防统方
- 防篡改

对外数据实时交互，实现沟通无界限
- 医保专线
- 市区域卫生信息平台
- 远程医疗云平台
- 网上报疫

建立综合管理平台，支持领导决策
- 数据分析、监控系统
- 质量指标检测分析平台
- 医务管理系统
- 医院精细化管理

目前超过90个业务系统，超过20个合作公司


VIRUS
CRACKER
INTRUDER
SPYWARE
PASSWORD
IDENTITY
CODE
UNSAFE
THEFT
HACKER

02

建设实践

医院信息安全建设步骤

01 **需求**

评审要求硬性指标、等保要求、发现新问题

02 **选型**

找到解决办法、测试、试用

03 **申请经费**

价格评估、要钱

04 **设备正式部署**

制定策略、逐步推进

05 **维保升级**

—— 与系统建设步骤类似，但成果展示方式不同

医院信息安全威胁(传统)

物理环境：

机房安全（温度、湿度、静电、防雷、防火、防盗、电力供应）

服务器、存储等设备（冗余、容灾）

网络及终端安全：

双链路保障

木马与病毒、操作系统漏洞、黑客攻击

应用及数据安全：

权限设置、密码机制、身份验证、数据丢失、篡改及泄露

医院信息安全威胁(新)

医改对医院信息共享、远程医疗协助的政策导向，延伸出的信息安全保障需求（无线网络、掌上医疗、远程医疗）

医院信息系统互联互通的实现，使得医院信息系统面临更多来自外部的威胁（内网、外网）

新技术的应用产生新的安全隐患（大数据、云桌面、虚拟化、集成平台）

防疫常态化后外部环境的变化

医疗设备的远程维保、电视等显示屏的遥控功能

——融合、协同、跨界惹的祸

等级保护

等级保护是唯一出路（备案、差距测评、整改、验收）

系统分类

（互联网医院、平台需要独立）

等级保护不同级别对设备要求不同

二级等级保护

产品	是否必须	备注	预算金额（万元）
防火墙	必须	部署位置：互联网出口边界，服务器区边界，分院区边界，医保、政务网边界各1台	30
入侵检测	必须	核心交换机镜像端口旁路	30
防毒墙	必须	部署位置：互联网出口边界，服务器区边界，分院区边界，医保、政务网边界各1台，或者使用防火墙上的防毒墙模块	30
网络版杀毒软件	必须	按1800点计算	50
日志审计系统	必须		30
WAF	必须		25
备份系统	必须		60
准入系统	建议	按1800点计算	60
数据库审计	建议		25
堡垒机	建议	授权数150个	30
合计			370

三级等级保护

产品	是否必须	备注	预算金额（万元）
防火墙	必须	部署位置：互联网出口边界，服务器区边界，分院区边界，医保、政务网边界各2台	30
入侵防御	必须	部署位置：互联网出口边界，服务器区边界，分院区边界，医保、政务网边界各2台，或者使用防火墙上的入侵防御模块	30
防毒墙	必须	部署位置：互联网出口边界，服务器区边界，分院区边界，医保、政务网边界各2台，或者使用防火墙上的防毒墙模块	30
网络版杀毒软件	必须	按1800点计算	50
日志审计系统	必须		30
WAF	必须		25
上网行为管理	必须		30
准入系统	必须	按1800点计算	60
数据库审计	必须		25
堡垒机	必须	授权数150个	30
备份系统	必须		60
容灾系统	必须		200
桌面管理	建议	统一管控办公计算机的使用规范，便于安全管理员对终端的运维	40
流量分析	建议	用于提升网络使用效率，优化关键业务体验，划分运维职责。	50
漏洞扫描	建议	发现现网中可能存在的漏洞	30
负载均衡	建议	互联网出口部署2台链路负载均衡，业务服务器区前端部署2台业务负载均衡	40
网闸	建议	保证两套系统之间没有直接的物理通路，以达到隔离与交换的目的。	30
态势感知	建议	实现对网络攻击特别是新型网络攻击行为的分析，部署后可以提升等保分数	150
防泄密	建议	网络出口处部署网络DLP、邮件DLP，业务电脑上可部署终端DLP	40
数据脱敏	建议	业务系统上可使用动态脱敏，测试区调用数据使用静态脱敏	60
VPN	建议	使用VPN让外地员工或者运维人员访问到内网资源	30
合计			1070

最基础产品

产品	等保三级是否必须	主要功能	实施优先级
防火墙	必须	在不同密集的网络间部署防火墙，实现区域划分以及访问控制等功能，实现不同区域之间的防护。	一级，防火墙还具备入侵防御和防病毒功能，同时可以保障各区域之间的业务系统免受到外部的攻击，以及阻断恶意文件的传播
入侵防御	必须	通过串接或者端口镜像的方式部署在网络中，发现可疑传输时发出警报或者采取主动反应措施的网络安全设备	一级，在网络中部署入侵检测系统。实现入侵检测功能。另外，可以使用防火墙中的模块代替
防毒墙	必须	防毒墙部署在医院局域网和互联网交界的地方。用于对网络传输中的病毒进行过滤的网络安全设备。阻止病毒从互联网侵入内网。	一级，在边界部署防毒墙，实现恶意代码防护功能。另外，可以使用防火墙中的模块代替
网络版杀毒软件	必须	在安全管理区部署网络版防病毒控制台，网络版杀毒软件系统由控制中心和终端两部分组成，将系统的管理端部署在运维管理区，防病毒终端部署在需要被保护的服务器或者终端，执行最终的杀毒扫描、入侵防御等安全操作。并向安全控制中心发送相应的安全数据。	一级，在医院计算机上部署杀毒软件，实现恶意代码防护功能。
日志审计	必须	安全管理区部署台日志管理系统，统一收集网络中各安全设备、网络设备、主机系统、应用系统日志，实现日志的集中式存放，确保留存6个月以上。	一级，使用日志审计系统实现日志的集中式管理和存放。
准入系统	必须	网络准入管理解决方案是通过定义一个可信域，允许可信域内的计算机互相访问，而禁止非可信域内的计算机与可信域内的计算机进行通讯，从而杜绝任何形式的非法入网，彻底防止非法计算机利用直插网线、仿冒内网合法计算机IP和计算机名、直连网内合法计算机、私接路由这些常见和难以管理的方式违规入网。	一级，可以通过交换机配置IP绑定MAC地址实现访问控制策略，但是配置复杂，不便于管理，因此部署使用准入系统。
备份系统	必须	数据备份是为了防止由于操作失误、系统故障等人为因素或意外原因导致数据丢失，而将整个系统的数据或者一部份关键数据通过备份保存在其他地方。	一级，通过数据备份系统满足重要数据的备份与恢复功能；
容灾系统	必须	当计算机系统在遭受如火灾、水灾、地震、战争等不可抗拒的自然灾难以及计算机犯罪、计算机病毒、掉电、网络/通信失败、硬件/软件错误和人为操作错误等人为灾难时，容灾系统将保证用户数据的安全性（数据容灾）	一级，搭建异地容灾系统，实现重要数据处理系统的热冗余，保证系统的高可用性。

重要产品

产品	等保三级是否必须	主要功能	实施优先级
数据库审计	必须	通过端口镜像的方式获取流量，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警。它通过对用户访问数据库行为的记录、分析和汇报，来帮助用户事后生成合规报告、事故追根溯源	一级，可以开启数据库本身的审计功能，但是会对数据库的性能和存储造成较大的负担，因此部署数据库审计系统来实现等保的数据审计功能
堡垒机	必须	在安全运维管理区部署堡垒机，在一个特定的网络环境下，为了保障网络和数据不受来自外部和内部用户的入侵和破坏，而运用各种技术手段实时收集和监控网络环境中每一个组成部分的系统状态、安全事件、网络活动的服务器，以便集中报警、及时处理及审计定责。	一级，可以通过ACL访问控制策略和主机基线，权限配置实现，访问控制和安全审计功能，但是配置复杂，不便于管理，因此部署堡垒机
WAF	如涉及到网站则必须	对外发布业务区部署WAF，实现漏洞攻击防护:网站安全防护目前可拦截常见的web漏洞攻击,例如SQL注入、XSS跨站、获取敏感信息、利用开源组件漏洞的攻击等常见的攻击行为。	二级，如果等保对象是对外发布的网站，则需要部署WAF或者云WAF
上网行为管理	如涉及到上网用户则必须	在办公外网部署上网行为管理系统，主要是实现互联网访问的审计要求和流量管理，因此外网上网行为管理设备将部署在防火墙之后，通过流量审计分析与管理，实现网络资源使用管控的功能。	二级，如果等保的对象涉及用户上网，则需要部署上网行为管理对用户进行审计
态势感知	强烈建议	安全态势感知平台，分别从日志、网络流量两个方面对全网安全态势进行感知发现，及时为医院信息安全管理提供决策支持。	一级，使用态势感知对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析
桌面管理系统	建议	通过桌面管理，可以实现业务终端的补丁管理、使用安全配置、远程桌面协助等功能	二级，统一管控办公计算机的使用规范，便于安全管理员对终端的运维
流量分析系统	建议	部署流量分析系统能充分分析网络资源利用率，对分布式收集的流量信息进行统一的分析处理利用流量侦测对网络资源进行主动探测收集、分析整理、可视化界面输出	二级，为网络做一次全面体检，并给出诊断建议。用于提升网络使用效率，优化关键业务体验，划分运维职责。
漏洞扫描	建议	漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测行为	二级，漏扫部署的目的是发现现网中可能存在的漏洞，但无法自行修复，建议通过安全运维服务进行增补，实现漏洞发现、测试、修复加固的工作
负载均衡	建议	负载均衡实现对数据中心、链路以及服务器状态的实时监控，数据流的合理分配，使所有的数据中心、链路和服务器都得到充分的利用。可扩展应用系统的整体处理能力，提高其稳定性，切实改善用户的访问体验，降低IT投资成本。	二级，部署负载均衡保证网络各个部分的带宽满足业务高峰期需要
网闸	建议	网闸由两套各自独立的系统分别连接安全和非安全的网络，两套网络之间通过网闸进行信息摆渡，保证两套系统之间没有直接的物理通路，以达到隔离与交换的目的。	二级，按具体环境和业务需求而定，可对防火墙进行增补，满足重要网络区域与其他网络区域之间应采取可靠的技术隔离手段
防泄密	建议	在网络中部署DLP，实时发现、监控网络流量、终端信息数据中的敏感数据传输，可发现敏感数据泄密风险。	二级，使用数据防泄密系统，实现敏感数据外发发现或者阻断
数据脱敏	建议	署脱敏系统，通过屏蔽来保护数据。对敏感数据提供了实时的、以角色和权限为驱动的脱敏。	二级，使用脱敏实现禁止未授权访问和非法使用用户个人信息。
VPN	建议	部署使用VPN让外地员工或者运维人员访问到内网资源。外地员工在当地连上互联网后，通过互联网连接VPN，然后通过VPN进入医院内网。为了保证数据安全，VPN服务器和客户机之间的通讯数据都进行了加密处理。	二级，使用VPN保证重要数据在传输过程中的保密性

申请经费

每年部门预算

（最好每年有固定投入）

利用上级的发文

抓住每一次出现的小问题

（整改依据）

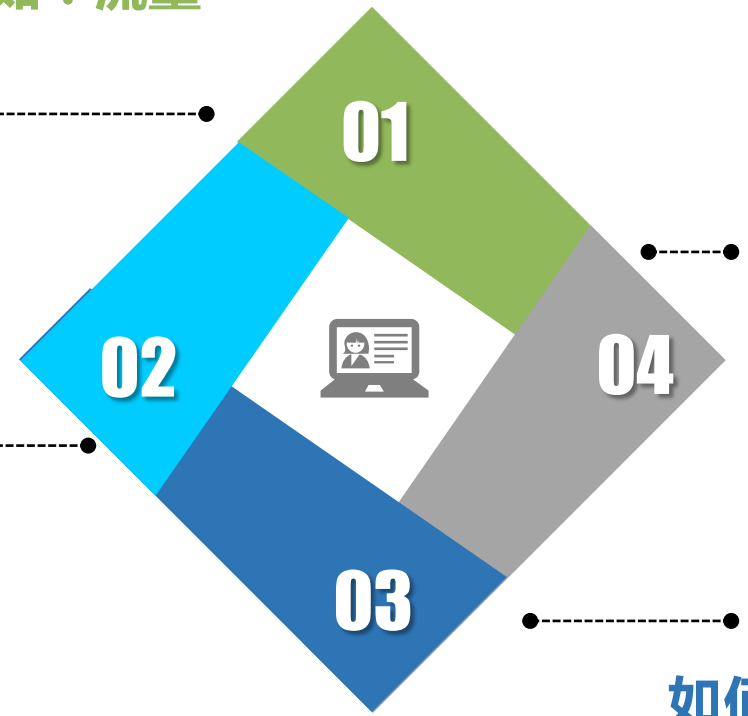
延迟测试时间

——心理博弈

设备选型

满足现在为主,展望未来为辅（如：流量控制设备）

考虑自身的维护能力（对公司的依赖程度、购买服务）



产品升级（软件、硬件）、扩展能力、维保年限（三年、五年）

跟终端有关的点数购买（按实际数量、并发数量）

考虑购买不同厂家产品（病毒库不同）

如何部署（测试：策略制定便捷性、工作量大小，如：白名单、黑名单、是否可以设置组策略）

——按等保要求，选合适自己的，小心陷阱

设备部署

联合公司根据医院业务制定策略

逐步推进，切不可一次到位

（分楼层、分业务，从松到紧）

策略做好备份

每个修改点都要做好测试

做好停机的准备，提前通知各部门


VIRUS
CRACKER
INTRUDER
SPYWARE
PASSWORD
IDENTITY
CODE
UNSAFE
THEFT
HACKER

03

建设误区

信息安全建设误区

01 安全建设应注重整体规划而非只看某一点：

信息化建设中应充分考虑信息安全，避免今后在安全运维中陷于 “头痛医头，脚痛医脚”疲于奔命的局面

02 建立安全管理制度的同时更应抓落实：

安全管理制度必须具备可操作性，定期回顾，找出不足，避免制度不到位、责任不明确，出现问题难以查找原因的局面

03 资金应分期投入而非一次性：

信息安全是一个长期的过程，非一朝一夕可以完成，也非完成后就可安枕无忧，必须形成周期性投入（产品迭代、服务周期）

04 不应只重视安全产品的采购，忽视产品应用：

购买产品需要前期充分论证，买合适自己的，借助（而非依赖）公司力量用好安全产品


VIRUS
CRACKER
INTRUDER
SPYWARE
PASSWORD
IDENTITY
CODE
UNSAFE
THEFT
HACKER

04

总结思考

外联平台的安全隐患

对外需要提供各种数据交互

- 如：医保（结算）、卫建委（区域医疗）、公安（患者信息上传）、上级部门（管理数据提取）
- 采用前置机+专线模式，注意：不要因为专线而轻视安全隐患。

对外

第三方平台的数据交互

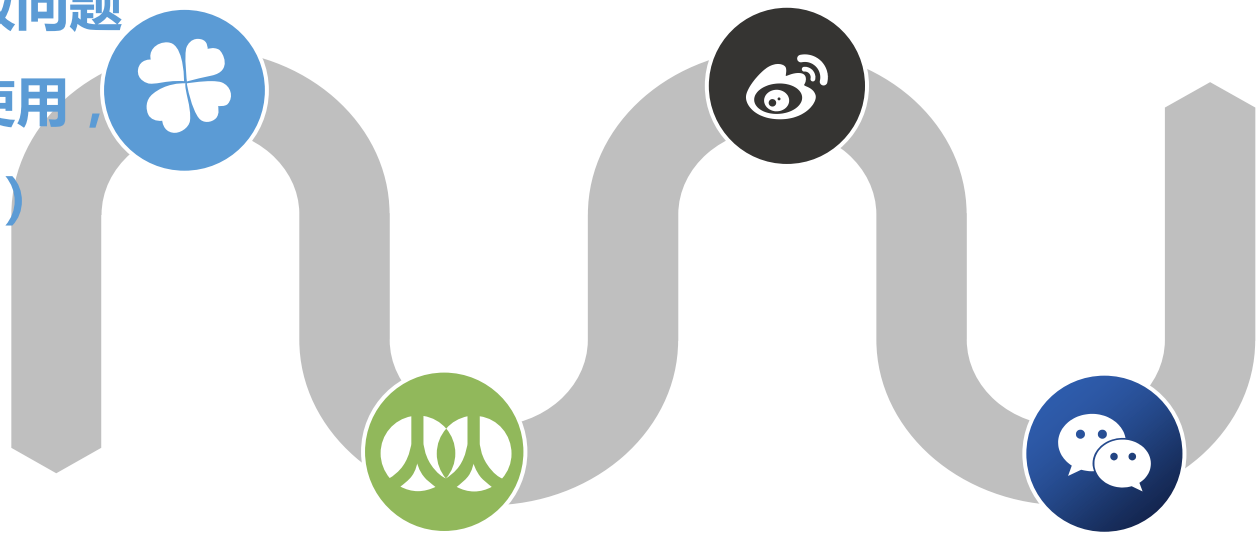
- 如：检验外送、药品配送
- 采用VPN加密通道模式，特点：存在一定的开发工作量，需要经费投入。

第三方

互联网业务引发的数据使用问题

如何解决数据使用授权，如：手机端患者绑定时身份核实、
检查检验查询权限（建议针对患者签订同意书、相关部门审批）

数据归属问题、数据存放问题
（境外不能放，邮箱的使用，
报废机器硬盘的处理）



针对行政科室人员：内外网开放通道（建议签订保密协议）

相关业务的开发公司工程师，通过VPN远程运维（建议签订保密协议）

——制定数据使用制度、相关人员签订协议

总结思考

信息安全是长期工作，
没有起点也没有终点

做好培训，定期应急演练
（电源在哪、设备在哪，哪个部门要干啥）

出现问题：控制范围、
及时处理（与网监建立联系）

——可以考虑购买安全服务，同时要避免被安全服务公司绑架

内忧外患时刻保持警惕
小心城门失火殃及池鱼