|  |
| --- |
| **附件：信息网络安全加固服务项目规格要求** |
| **序号** | **项目** | **要求** |
|  | 漏洞扫描和渗透测试服务 | 针对禹州市人民医院信息系统，从业务专网、互联网等位置利用各种手段对某个特定业务系统进行技术性渗透测试，发现和挖掘系统中存在的安全问题，使用专业检测工具和分析技术对院内信息系统进行漏洞扫描及渗透测试，发现信息系统服务器操作系统、数据库、中间件、网络及安全设备等存在的漏洞，并分析、评估漏洞风险程度，提供整改建议。并提供漏洞复测服务。服务期内包含对重要信息系统的渗透测试服务。根据漏洞扫描、差距分析等工作结果，结合院内信息系统业务需求，通过技术手段协助院内对信息系统相关的操作系统、网络与安全设备进行安全策略加强、调优，加强网络、系统和设备抵御攻击和威胁的能力，整体提高网络安全防护水平。 |
|  | 资产梳理服务 | 通过文档资料收集、访谈和现场勘查等方式，梳理信息系统现状，从整体上获取信息系统相关资料，并对所获取资料进行汇总分析，了解系统的功能、服务对象、安全保护属性、相关软硬件资产及重要程度、网络架构、系统部署、业务数据交互等具体情况。 |
|  | 应急响应技术支持 | 须明确一名信息安全技术专家，作为本次项目的应急响应团队负责人，在日常工作中为采购人提供7\*24小时信息安全技术咨询及工作建议。当采购人信息系统突发信息安全事件时，须及时组织有解决问题能力的技术团队赶赴采购人现场，分析安全故障和事件原因、形成处置计划、处理安全故障并协助恢复系统正常工作。在事件处理完毕后及时出具突发事件应急服务处置报告。响应时间要求如下：1) 响应时间：30分钟以内；2) 到场时间：4小时内到达现场；3) 处置时间：12小时内处置完毕并出具处置报告。 |
|  | 重要时期安全保障服务 | 根据信息网络安全工作需要，提供重保安全技术支持，在两会、国庆等国家重要会议、节日期间，提供现场或远程的安全事件通报、安全加固整改及7\*24 安全监控与应急响应服务；配合公安机关、网信部门每年对医院进行的网络安全检查工作。 |
|  | 网络安全培训服务 | 通过大量的当前典型网络安全事件导入，对网络安全威胁给予直观描述，加强员工安全意识，尤其防范社会工程学攻击。包括全员安全意识宣传、内部安全意识培训以及第三方安全意识宣贯等。 |
|  | 网络安全加固服务 | 对核心业务系统按照最新标准进行网络安全差距分析，根据差距分析结果对安全漏洞进行加固、安全缺陷进行弥补、安全策略进行调整、安全管理进行提升，确保经过等级保护安全加固使各核心业务系统（HIS、LIS、PACS、EMR）达到相应级别的等级保护标准（三级）要求。 |
|  | 业务系统安全加固及达标检测服务 | 按照采购方要求对医院核心业务系统进行安全加固、性能测试、优化升级、接口开发、运行维护及综合技术支持服务，完成核心业务系统（HIS、LIS、PACS、EMR）的网络安全达标检测（满足等保三级要求）并取得证明文件。 |