**服务项目内容及服务要求**

**一、比选项目内容一览表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务项目** | **服务内容** | **单位** | **数量** | **备注** |
| 1 | 资产梳理 | 通过数据发现与评估系统，结合人工服务，对医院的网站和内部资产进行自动化识别和梳理，形成可视化图形表，为医院提供全面的资产清单。 | 2次/年 | 1 |  |
| 2 | 定期漏洞扫描 | 一、服务描述：使用系统漏洞扫描工具对数据库、操作系统、中间件等进行漏洞、端口、弱口令扫描，扫描完成后由技术人员对漏洞进行确认测试，提出整改建议，协助开发人员整改。二、具体服务内容：a.准备阶段 对目标用户的服务范围内资产进行搜集，获取域名、IP、网络拓扑等相关信息，作为后续的扫描资产范围； 签署漏洞扫描委托授权函，获得用户的授权； 约定漏洞扫描的时间和漏洞扫描工具；评估漏洞扫描过程中可能存在的技术问题并与用户协商应急响应策略；与用户沟通相关的网络环境，提供漏洞扫描设备接入点；与用户协商进行相关目标资产文件与数据的备份；b.扫描实施阶段 实施扫描阶段开始现场检查网络连通性情况，根据情况分配合理 IP，确保扫描工具能探测到扫描范围内的所有主机，且无防火墙等安全设备进行阻拦，之后开展漏洞扫描； 扫描过程中，如果目标系统出现无响应、中断等情况，扫描人员会立即中止漏洞扫描，并配合客户进行问题排查，在确认问题以及完成系统修复之后，根据分析结果调整扫描方式，经客户再次授权同意的前提下才会继续进行其余的扫描；c.总结汇报阶段 总结项目工作内容及成果，并向客户汇报扫描报告结果。三、服务交付物《漏洞扫描报告》 | 4次/年 | 1 |  |
| 3 | 渗透测试服务 | 对3个核心业务系统进行渗透测试 | 2次/年 | 1 |  |
| 4 | 日常巡检 | 对服务器设备、网络设备、安全设备进行定期巡检 | 12次/年 | 1 |  |
| 5 | 维保升级维保 | 超融合集群、网络/安全设备升级及维保服务 | 1项/年 | 1 |  |
| 6 | 制度完善服务 | 协助完成政策动所需的管理制度的梳理及补充工作 | 2次/年 | 1 |  |
| 7 | 安全培训 | 为增强医院人员的安全意识、提升全员的网络及信息安全知识，通过当前典型的安全事件导入，定期开展信息安全宣传活动，宣传内容包括：网络及信息安全法律法规、员工安全意识、网络及信息安全制度等 | 2次/年 | 1 |  |
| 8 | 安全策略调优 | 协助进行安全策略配置检验，并针对性对安全设备上安全策略配置进行相关优化 | 4次/年 | 1 |  |

**二、服务要求**

### **（1）资产清单梳理服务**

完成我院资产清单梳理，全面对数据名称、数据内容、确定存储位置、数据流向、使用方式进行梳理，并对每个内容进行明确，完成对资产及数据进行清晰化、定位化。借助安全工具对当前信息资产进行全面发现和深度识别，并结合人工梳理成真实、可用的资产台账。

### **（2）漏洞扫描服务**

对我院数据库、操作系统、中间件等进行漏洞、端口、弱口令扫描，扫描完成后由服务商及我院技术人员对漏洞进行确认测试，以系统（网络、电脑终端、HIS、LIS、PACS系统等）为单位输出报告，提出整改建议，协助开发人员整改。

整个安全漏洞扫描服务的流程分为三个阶段，准备阶段、扫描过程和报告汇报。通过这三个阶段，结合安全漏洞扫描内容和实际客户系统情况，完成安全漏洞扫描服务。

准备阶段:前期技术交流包括相关安全扫描技术，扫描原理、描方式及扫描条件进行交流和说明:同时商谈安全漏洞扫描服务的范围，主要是哪些主机，网络设备，应用系统等:并结合实际业务情况需求，确定扫描范围，扫描实施的时间，设备接入点，IP地址的预留，配合人员及其他相关的整体漏扫方案。

扫描过程:依据前期准备阶段的漏扫方案，进行漏洞扫描、漏洞分析和漏洞测试，扫描过程主要是进行范围内的漏洞信息数据收集，为下一步的报告撰写提供依据和数据来源。漏洞扫描，主要采用远程安全评估系统进行范围内的安全扫描。漏洞分析，主要是对扫描结果进行分析，安全工程师会结合扫描结果和实际客户系统状况，进行安全分析。漏洞验证，对部分需要人工确定和安全分析的漏洞，进行手工测试，以确定其准确性和风险性。

报告与汇报:这个阶段主要对现场进行扫描后的数据进行安全分析，安全工程师对远程安全评估系统输出的报告，漏洞分析结果及漏洞测试具体情况进行综合梳理，分析，总结。最后给出符合客户信息系统实际情况的安全需求的安全建议。

### **（3）渗透测试服务**

3个核心业务系统的渗透测试:利用各种主流攻击技术对授权指定的应用系统做模拟攻击测试，找出安全风险点，出具渗透测试报告，并给出风险点整改建议，协助我院及相关系统开发人员进行整改。

### **（4）月度巡检服务**

对服务器设备、网络设备、安全设备进行定期巡检。巡检内容包括硬件状态、配置备份、补丁更新。

### **（5）网络设备维护服务**

特征库和维保具有一定的时效性，目前防火墙、超融合、交换机特征库有效期和维保时间已到期，为使网络设备发挥最大功效，需对对应产品功能软件进行升级，保证安全产品能及时更新厂家最新发布的漏洞特征库，从而进行实时有效的安全防护，并且为设备硬件提供一年的维保服务，当设备故障时，对设备进行现场维修或免费返厂维修。指派专业人员进行升级，实施完成形成报告提交贵单位，设备维修过程遇到任何风险问题先向单位请示再操作，以最快速度解决问题以免影响业务。

### **（6）安全设备维护服务**

安全产品本身提供了全面的信息网络安全防护保障方案，但各类软件、应用系统本身所存在的安全漏洞隐患却在不断的被不法分子挖掘并进行恶意利用，攻击手段在不断的更新。作为安全产品如果不能及时升级进行更新，也就失去了对最新的恶意网络行为及系统漏洞进行及时有效识别和分析的能力，从而导致信息资产安全风险大大增加。

在服务期内，解决日志审计系统提供同等功能软件的升级和在正常使用下发生非人为故障或质量问题，负责返厂维修。指派专业人员进行升级，实施完成形成报告提交贵单位，设备维修过程遇到任何风险问题先向单位请示再操作，以最快速度解决问题以免影响业务。