**赣州市中心血站网络安全服务项目**

**采购需求**

1. **采购项目：**赣州市中心血站网络安全服务三年
2. **采购需求**

（一）响应供应商须提供具有中国网络安全审查技术与认证中心颁发的信息安全应急处理服务资质证书复印件并加盖响应供应商公章；需具备安全运维服务经验，自2022年01月起（以签订合同时间为准）承担过至少3份类似安全运维服务项目业绩，须提供中标（成交）通知书或合同原件彩色扫描件并加盖响应供应商公章进行佐证。

（二）所有服务的知识产权问题，由响应供应商自行负责。

（三）本采购需求提出的是最低限度的要求，响应供应商的方案应达到或优于本要求，且符合国家有关标准和规范要求。

（四）成交供应商须保证对本项目实施中所获得任何资料和信息严格保密，并与采购人签订保密责任书。成交供应商对相关工作所涉及的国家秘密和商业秘密负有保密责任，对相关工作所产生的信息资料负有保密义务，严禁复制、拍摄、摘抄、泄露、贩卖国家秘密、商业秘密，严禁未经许可披露或私自泄露相关工作所取得的任何资料和谈话内容。如有违反保密要求之行为的，应承担相应法律责任并赔偿由此产生的所有损失。

（五）服务清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务类型** | **服务名称** | **服务内容** | **运维频率** | **输出物** |
| 1 | 安全托管服务 | 安全托管服务 | 1. “安全托管平台”的告警数据支持与云端运营中心联动，云端安全专家提供7\*24小时服务。   2、发生相关风险告警，可通过钉钉、微信、短信或电话等形式及时通知用户，并第一时间进行有效的阻断清除，并做好风险总结报告。 | 7\*24小时 | 《巡检报告》/月 |
| 2 | 安全梳理 | 资产梳理 | 主要梳理内容包括物理环境、网络拓扑，网络设备、安全设备、系统服务器、设备接口互联及陈列情况，补齐线路互联标识等。 | 每季度 | 《资产台账》/季度 |
| 业务梳理 | 根据业务流程，主要梳理内容包括安全设备的管理方式，网络及安全设备的策略配置，通过访谈、收集并分析相关设备的配置，梳理业务走向。 | 每季度 |
| 制度梳理 | 根据等级保护三级要求，完善各项信息安全管理制度，通过对制度的补充、完善，形成一套可以满足信息安全等级保护三级要求，并且可以实际运用的管理制度文件。 | 每年 | 《安全管理制度汇编》/年 |
| 4 | 日常运维 | 巡检服务 | 全面检查，对信息系统所涉及的物理环境、网络和安全设备运行状况、系统服务器和相关安全设施进行全面和严格的专项巡检。包括设备版本与基本配置、设备资源使用状态、接口配置与状态、访问控制策略、告警信息、系统配置策略等关键工作指标进行例行监控。 | 每月 | 《巡检报告》/月 |
| 病毒查杀 | 通过专业的安全软件或工具来扫描、定位业务系统服务器及客户端中的病毒及恶意软件，提供修复建议，并协助修复。 | 每月 |
| 故障处置 | 巡检过程中，发现设备故障后，为了确保业务系统的持续运行，依据应急处置流程对故障进行处置。 | 按需 |
| 安全通告 | 定期提供最新病毒的防御方案、最新系统漏洞信息及其修复方法、最新发生的安全事件等内容的安全通告报告。 | 每月 |
| 5 | 安全检测 | 基线检查 | 根据既定的检查规范及方法，采用人工检查用表（checklist）、脚本程序或基线扫描工具对评估目标范围内的主机系统安全、数据库安全、中间件安全等进行系统的策略配置、服务配置、保护措施以及系统和软件升级、更新情况，是否存在后门等内容进行检查，识别潜在的风险，提供修复建议，并协助进行漏洞修复。 | 每月 | 《巡检报告》/月 |
| 漏洞扫描 | 采用行业认可、安全合规的漏洞扫描系统，通过定制的扫描规则，形成安全扫描策略文档，对服务器、网络设备、安全设备等进行自动化安全扫描，输出安全扫描报告提供修复建议，并协助进行漏洞修复。 | 每月 |
| WebShell扫描 | 通过web后门检查工具，针对网站或应用系统服务器所有文件进行安全扫描，发现系统文件中潜在的webshell、网页后门等恶意文件，提供修复建议，并协助进行漏洞修复。 | 每月 |
| 漏洞加固指导服务 | 基于攻防视角评估资产漏洞风险，识别可实际产生风险的漏洞，提供漏洞修复的优先级建议，可大幅减少漏洞整改工作量。 | 每月 |
| 漏洞无效化服务 | 对于无法整改的漏洞，提供漏洞无效化技术手段：可使扫描器扫得到资产，但无法扫描到漏洞。 | 每月 |
| 7 | 优化加固 | 网络安全优化加固 | 优化加固是指采取一系列措施来增强网络环境的安全性，以抵御各种潜在的威胁和攻击。主要针对网络设备、安全设备、服务器、应用系统以及网络结构的口令策略、账户权限、网络服务、访问控制、用户鉴别等加固项进行加固，包括关闭非必要的服务和端口、设置强密码策略、合理配置硬件设备的访问控制列表、分析网络架构和拓扑，评估网络的安全性和可扩展性等，通过该服务制定详细的安全策略和实施规范，减少网络环境中潜在的安全风险和攻击威胁。 | 每月 | 《巡检报告》/月 |
| 8 | 网络安全应急演练 | 模拟演练 | 针对应急预案中全部或大部分应急响应功能，搭建模拟测试环境，演练过程采取交互方式进行，要求尽量真实，以测试应急响应的功能。例如，指挥和控制功能的演练，检测、评价多个部门在紧急状态下实现集权式的运行和响应处置能力等。 | 一年1次 | 《网络安全应急演练工作方案》 《网络安全应急演练总结报告》 |
| 9 | 渗透测试 | 渗透测试 | 通过模拟黑客使用的工具、分析方法对网站、业务系统、应用系统等进行安全测试，并结合智能工具扫描结果，由高级工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。主要分析内容包括WebShell、注入、逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误以及其他专项内容。通过模拟真实的攻击场景，识别潜在的安全风险，提供修复建议，并协助进行漏洞修复。提高网站及业务系统的安全性。 | 一年1次 | 《渗透测试报告》 |
| 10 | 风险评估 | 信息系统技术评估 | 信息系统安全风险评估从风险管理角度，运用科学的方法和手段分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，防范和降低信息安全风险，使风险控制在能接受的范围内。主要包含信息系统资产，弱点/脆弱性、威胁和风险四个要素。包括： 1.对信息系统资产进行识别，并对资产的价值进行赋值； 2.对脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值； 3.对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值； 4.根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性； 5.根据脆弱性的严重程度及安全事件所作用的资产的价值计算安全事件造成的损失； | 3个系统 | 《风险评估报告》 |
| 安全管理评估 | 主要从以下几方面分析被评估信息系统安全管理状况：管理机构、管理制度、人员管理、系统建设管理和系统运维管理，为后续脆弱性分析及综合风险分析提供参考数据。安全管理评估可采用问询、调查问卷和现场观察等方式进行。 |
| 11 | 网络安保服务 | 重保服务 | 针对国家规定的法定节假日、重大会议、政治活动等其它具有广泛影响的活动，派遣高级安服人员，以现场或远程值守的方式提供网络安全保障服务，协助处理信息安全事件。包括前期重要业务的检查、安全扫描、网络安全加固等准备工作，确保在重要敏感时期的网络安全。 | 按需 | 《重保安全服务实施方案》 《重保安全服务实施报告》 |
| 12 | 应急响应 | 应急预案 | 根据信息系统及其承载业务信息的重要性，以及业务特点，结合国家、地区和行业等信息安全政策和标准，协助用户制定应急预案，明确应急响应以及预防、预警机制，针对可能的安全事件编制规范的应急处理流程。 | 一年1次 | 《网络安全应急预案》 |
| 应急响应 | 10人以上应急保障团队，提供7\*24小时响应服务，普通问题需2小时内解决，如需现场服务需0.5小时内派出专业应急响应工程师到现场，主要包括（不限）以下情况的应急响应： 1、网络、安全、系统、服务器及涉及到的物理环境、消防、精密空调、UPS等所有设备设施软硬件的故障处理及维护调试。 2、勒索病毒事件应急响应：对染毒主机进行排查，对当前环境进行风险排除与主机加固，处置取证后提供专业完整的应急响应报告，协助解决因勒索病毒所造成的的重要业务瘫痪、重要数据被加密等情况，减少因勒索病毒所造成的巨大经济损失。 3、数据泄露事件应急响应：对数据库操作和查询日志、服务器进程、服务器和网络日志、可疑文件等进行排查，并作应急处置，处置完成后对存在问题的系统或数据库提出点对点的整改加固方案，防止数据二次泄露。 4、Web安全事件应急响应：对受影响系统进行全面威胁排查，Web漏洞特征分析，包括Sql注入特征、文件上传特征、命令执行特征、Windows/linux恶意命令攻击特征、框架漏洞特征、中间件特征等，协助修复漏洞以防同类安全事件再次发生，尽快使网站系统恢复正常运行，减少因安全事件造成的经济损失。 | 按需 | 《网络安全事件应急处置报告》 《网络维护报告》/每月 |
| 13 | 安全培训 | 安全意识培训 | 面向单位全员开展专业的网络与信息安全意识培训，提高受众个人隐私保护、常规攻击防护、信息安全管理等能力，增强个人网络安全防护意识，规避网络攻击风险。 | 一年1次 | 《安全意识培训PPT》 |

（六）项目服务考核要求

|  |  |  |
| --- | --- | --- |
| **序号** | **考核内容** | **分值** |
| 1 | 关键业务系统发生网络安全事件，造成不良影响，出现一次扣10分 | 10 |
| 2 | 关键业务系统发生网络安全事件，被上级监管部门通报，出现一次扣20分 | 20 |
| 3 | 因技术服务人员不具备相应的工作能力，导致网络安全问题而影响业务的，出现一次扣5分 | 5 |
| 4 | 未按操作规范及时提供相应交付文档或者提供的交付文档不满足考核单位、上级部门要求的，出现一次扣5分 | 5 |
| 5 | 因技术服务人员工作态度不端正，被考核单位投诉的，出现一次扣5分 | 5 |
| 6 | 未按要求安排专业人员现场保障，出现一次扣5分 | 5 |
| 7 | 未按计划积极开展各项工作，出现一次扣5分 | 5 |
| 8 | 发生安全事件未按时到现场处理，出现一次扣5分 | 5 |
| 9 | 未按合同约定履行服务内容，出现一次扣5分 | 5 |
| 10 | 响应时间，年度内未按甲方服务要求在规定时间内及时响应，出现一次扣5分 | 5 |

注:1、每扣1分扣500元，扣分上不封顶。

2、采购人对中标人的服务情况定期进行考核。考核后采购人将考核结果告知中标人，中标人应在收到考核结果五个工作日内进行确认，超时未确认且未提出异议的视同中标人同意考核结果。

（七）项目服务期限：合同签订后三年。