项目要求

1. **建设目标**

1.确保校内系统的身份认证机制和访问控制系统具有较高的安全性，只有经过授权的用户能够访问相应的敏感信息和系统功能。

2.提高校园系统对学生和教职员工个人数据的隐私保护水平，确保信息处理符合相关法规和合规性要求。

3.通过对信息系统进行全面梳理，并实施网络安全等级测评，排查网络安全隐患和薄弱环节，逐步完善网络安全管理制度和技术措施，增强网络安全防护能力，保证合法合规。

1. **建设方案**

### 对校园网站综合、自动化办公、智慧三全APP及信息门户四个系统开展信息安全等级保护测评，分别包括信息系统梳理及定级、信息系统测评及备案、安全管理情况的评估、技术防护情况的评估和系统整体安全情况评估。满足符合国家规定和标准规范，发现安全问题，确定建设整改需求，符合公安机关、行业主管部门监管要求，规避责任风险等。

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **技术指标** |
| **1** | **等级保护测评服务** | 参照国家等级保护2.0技术标准对我单位信息系统按照等级保护第二级标准开展测评和差距分析，出具整改意见和测评报告，完成系统定级专家评审工作，自合同签订之日起10个工作日内完成本次测评报告在网安部门的备案工作，并取得四个系统（网站综合、自动化办公、智慧三全APP及信息门户）有效的备案证明。  |
| 要求与《信息安全等级保护管理办法》（公通字[2007]43号）、《信息安全技术 网络安全等级保护实施指南》和《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]1429号）（含附件）等公安部信息安全等级保护系列文件要求保持一致。 |
| 要求测评包括IT网络设备、主机系统、应用系统、安全设备等。具体安全技术测评包含安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等五个层面；安全管理测评包括：安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理等方面的安全控制测评对10个大类进行测评。 |
| 在网络与信息安全专项保障和检查工作时，排查网络边界、数据、应用安全，确保重要网络和应用系统运行正常。对信息系统进行日志分析，形成每日攻击分析报告，针对网络中存在的高风险攻击行为进行影响分析，制定防范措施。跟踪收集最新的安全通告，漏洞通告、病毒通告等，针对系统漏洞及攻击情报协助对网络及主机进行安全加固工作。针对网络安全类突发事件进行应急响应，快速处置及恢复。对整体网络和信息系统进行实时保障，形成科学、有效、反应迅速的应急工作机制，确保特殊时期重要信息系统的实体安全、运行安全和数据安全，最大限度地减轻网络与信息安全突发事件的可能。 |
| ★交付物：信息系统等级保护测评报告。 |
| **2** | **渗透测试服务** | 针对等保测评系统由安全工程师现场部署渗透环境，通过真实模拟黑客使用的工具、分析方法来对网站进行模拟攻击，并结合智能工具扫描结果，进行深入的人工测试和分析，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、异常错误等以及其他专项内容测试与分析。渗透测试后出具正式的分析报告和解决方案，针对渗透测试出的问题、漏洞、缺陷等，完成整改及后续验证工作，每项渗透内容报告需要包括问题整改和验证的过程记录及详细的解决方案。 |
| ★交付物：渗透测试报告 |
| **3** | **漏洞扫描服务** | 对被测信息系统所涉及的主机服务器及相关网络设备、操作系统、数据库等进行安全漏洞扫描，收集漏洞扫描的结果，并通过人工验证掌握系统安全现状并提出漏洞分析报告。具体包括漏洞扫描、漏洞修补、漏洞复查等，确保漏洞管理工作实现从“漏洞发现”到“漏洞治理”的集中防护转变。 |
|  |  | ★交付物：漏洞扫描报告 |
| **4** | **网站检测服务** | 1、定期检查网站可用性，模拟用户访问定期访问目标网站。如发现网站故障、无法建立连接、状态码非200或网页内容加载超过15秒时，触发告警机制；可用性告警触发之后，应用会关闭3天内同网页相同类的告警，避免对用户产生过多的告警而造成打扰。如果这期间网站恢复了告警会重新开启可触发状态。2、★网站监控成功后，将默认的网页内容设为正常状态。定期对比监测的网页内容与正常内容，如发现不一致，立即触发告警。保障网站稳定运行。★通过周期性的监控，持续对网站的文本内容进行检测，以保障网站的安全性和合规性。一旦检测到敏感关键字的存在，则发出告警。★提供多个敏感词字典：内置字典、AI 智能检测引擎、自定义字典，触发告警时会提供网页快照，且高亮关键字；★发现网页中存在错链、坏链、异常友链等异常链接情况，则发出告警。★通过检测网站的文件和代码，识别潜在的挂马行为。一旦发现挂马现象，立即向用户发送告警通知。3、网站监测支持多种告警方式：站内信告警、邮箱告警、★微信通知告警、★钉钉机器人告警、★企业微信机器人告警。★通过检测网站的文件和代码，识别潜在的挂马行为。一旦发现挂马现象，立即向用户发送告警通知。★发现网页中存在错链、坏链、异常友链等异常链接情况，则发出告警。★平台可自动生产监控周报，每周一自动生成上一周期（上周一 00:00:00至上周日 23:59:59 ） |
| **5** | **其它** | 1、项目实施团队人员应具有相关资质证书，能顺利完成测评工作，具体如下：（1）中级测评师1名以上；初级测评师2名以上；测评师应至少一名具有工业和信息化部教育与考试中心颁发的网络安全威胁分析师证书；（2）项目经理同时具备高级测评师证书、信息安全保障人员认证证书（风险管理）、网络安全能力认证培训讲师（CCSC）证书、数据安全工程师证书；2、合同签订10个工作日内完成本次测评报告在网安部门的备案工作，每逾期一天扣10%的中标费用。3、投标公司应具备不得低于3份在新乡市类似的业绩合同。 |