上海市长宁区教育局文件

长教计〔2021〕12号

长宁区教育局关于增设部分信息化项目的函

长宁区科委:

一、理化实验室考试项目等级保护测评专项经费

长宁区教育局根据《上海市教育委员会关于做好2021年初中理化试验操作考试运行保障工作的通知》〔2021〕17号文件，教育局现急需加快考场建设和系统部署运行。依据GB/T22239-2019信息系统安全等级保护基本要求安全标准中重要系统的安全保障要求，需对“长宁区理化实验考试系统”、“长宁区理化实验考试智能赋分系统”开展安全等级测评工作（详见附件1）。中小学实验室考试系统安全等级测评项目经费所需经费12万元，动用历年项目资金承担。

二、教育安全专网主动防御系统项目经费

根据教委对教育专网安全等级保护的要求，长宁教育信息中心完成了教育专网三级等级保护的测评，根据测评报告整改建议以及等级保护测评 2.0 要求，需要部署主动防御系统。通过在长宁教育专网内部署主动防御系统后，系统可以提供面向业务层的主动防御，高效甄别伪装和假冒正常行为的已知和未知自动化攻击，为各类 Web、HTML5 提供强大的安全保护，防止攻击者对信息中心和学校的各类网站和应用进行破坏和攫取，保障学校网站和教育教学应用安全运行和数据安全（详见附加 2）。教育安全专网主动防御系统项目经费所需经费 35 万元，动用历年项目资金承担。

妥否，请函复

附件：1. 理化实验室考试项目等级保护测评项目需求

2. 关于教育安全专网主动防御系统的建设方案

长 宁 区 教 育 局

2021 年 4 月 19 日

(联系人：诸瑶涵，联系电话：22050766)

附件 1

理化实验室考试项目等级保护测评项目需求

一、采购技术要求

安全等级测评服务:

依据 GB/T22239-2019《信息系统安全等级保护基本要求》安全标准中二级系统的安全保障要求，分别对《长宁区理化实验考试系统》（4 个子系统，1 个区级机房，9 个学校机房、不超过 40 台服务器及安全设备）、《长宁区理化实验考试智能赋分系统》（3 个子系统，1 个区级机房，不超过 10 台服务器及安全设备）这两个应用系统开展安全等级测评工作，具体要求如下:

1、测评内容要求:

（1）技术要求

安全物理环境: 针对系统的机房、设备设施等对象进行核查;

安全通信网络: 针对系统的网络架构、网络设备、网络防护、通信传输等对象和内容进行核查和技术测试;

安全区域边界: 针对系统的网络架构、网络设备的安全区域边界防护情况进行核查和技术测试;

安全计算环境: 针对系统的网络设备、安全设备、服务器、重要客户端的操作系统和数据库、应用系统（如业务系统、办公系统、网站发布系统）等对象进行核查和技术测试;

安全管理中心：针对系统的网络架构、审计系统、运维管理平台等对象进行核查和技术测试;

渗透性测试：针对应用系统（如业务系统、办公系统、网站发布系统）等进行渗透性测试，内容包括网站远程扫描、参数过滤漏洞、远程权限控制、敏感信息泄露等;

（2）管理要求

安全管理制度：针对管理制度、制定和发布、评审和修订等情况进行核查;

安全管理机构：针对岗位设置、人员配备、授权和审批、沟通和协作、审核和检查等情况进行审核;

安全管理人员：针对人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理等进行核查;

安全建设管理：针对系统建设的全过程，系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发等进行核查;

安全运维管理：针对资产管理、介质管理、设备管理、监控管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理进行核查。

2、测评实施要求：

在安全等级测评工作中发现安全风险问题汇总后及时反馈用户单位，同时督促其实施问题整改。

待用户单位完成整改后，再对整改情况进行复核，以保证《长宁区理化实验考试系统》、《长宁区理化实验考试智能赋分系统》

两个系统安全性方面满足等级保护标准要求。

3、服务及文档要求

协助用户对其信息系统开展摸底调查，编制与填写被测信息系统的《定级报告》和《备案表》;

协助用户将信息系统定级材料递交至主管部门，通过备案审核;

提交完整的安全等级测评工作计划及测评方案;

初次现场安全测评完成后，分别出具两个系统的《测评问题汇总》;

全部安全测评工作完成后，分别出具两个系统的《安全等级测评报告》。

预算明细:

《长宁区理化实验考试系统》（4 个子系统，1 个区级机房，9 个学校机房、不超过 40 台服务器及安全设备）人民币柒万元整;

《长宁区理化实验考试智能赋分系统》（3 个子系统，1 个区级机房，不超过 10 台服务器及安全设备）人民币伍万元整。

共计人民币 120，000 元（拾贰万元整）。

附件 2

关于教育安全专网主动防御系统的建设方案

1.建设背景

随着国家对网络安全重视程度的提升，以及网络安全法的落地执行，教育网站正面临着越来越复杂的安全挑战。一方面，网页应用漏洞层出不穷，传统防护依靠不停的查补漏洞、更新规则，仍然无法避免亡羊补牢、疲于奔命的被动局面。另一方面，教育应用和数据不断向网站化迁移，教育网站面临着业务和数据安全的严峻挑战。学生数据倒卖者、黑客通过各种新型攻击手段和工具拥有绕过传统安全的防护，获取教职工、学生个人信息等敏感数据内容，极大的威胁了网站的数据安全。

2.建设目标

目前，长宁教育约 100 多个学校门户网站及重要的教学教育应用部署在长宁教育专网内，这些基于互联网的应用推动着长宁教育的现代化和信息化。但是，给教育教学带来进步和变革的同时，面临着各种来自互联网的攻击和风险。

为了确保暴露在互联网的学校门户网站和重要教学教育系统的安全运行，计划在长宁教育专网内部署一套主动防御系统来保护这些教育教学应用，通过部署主动防御系统，提升防御互联网自动化攻击能力，全面防止传统的 Web 漏洞攻击和新型自动化安全威胁，如漏洞扫描探测、零日漏洞攻击、撞库及暴力破解攻击、短信轰炸、网站克隆等，防止长宁教育专网内师生信息及敏感数据泄漏，最大限度的减少监管部门通报。

3.建设内容

通过在长宁教育专网内部署主动防御系统后，系统可以提供面向业务层的主动防御，高效甄别伪装和假冒正常行为的已知和未知自动化攻击，为各类 Web、HTML5 提供强大的安全保护，防止攻击者对信息中心和学校的各类网站和应用进行破坏和攫取，保障学校网站和教育教学应用安全运行和数据安全。

部署该系统后能在以下几方面增强长宁教育专网的网络安全:

（一）保障网站安全

防漏洞探测: 防止黑客通过漏扫工具扫描网站结构和应用漏洞。

防零日漏洞: 防止攻击者利用零日漏洞对系统发起攻击。

防应用 DDoS: 防止攻击者针对资源消耗高的业务批量发起自动化攻击。

（二）防止数据泄漏

防爬虫: 有效拦阻攻击者利用自动化程序爬取网站敏感信息、评论信息等内容。

防内鬼: 防止利用合法身份，通过工具批量窃取内部数据。

防数据遍历: 防止利用逻辑漏洞，通过工具批量导出学生及教师资料。

防拖库: 防止利用合法身份或盗用身份，通过脚本或者编制程序，模拟合法业务逻辑进行的批量信息导出。

（三）保护账号安全

防暴力破解: 防止对登录入口密码实施暴力破解。

防批量注册: 防止攻击者通过自动化工具进行批量注册。

防撞库: 防止黑客通过黑产数据库，利用自动化程序实施登

录尝试并盗取合法账号，进而获取用户敏感信息或进行欺诈。

（四）满足监管要求

网络安全法：防止攻击者通过正面攻击、模拟用户访问等方式获取用户数据;

网络安全等级保护制度 2.0：变被动防护为主动防护，变静态防护为动态防护，变单点防护为整体防控，变粗放防护为精准防护。

主动防御系统功能需求

序号	功能项描述
1	用户行为拦截：可以基于客户端的真人行为数据实现拦截，包括：键盘输入的次数、鼠标移动的次数、鼠标点击的次数、触摸板开始触摸的次数、触摸板滑动的次数，实现针对性拦截。
2	客户端环境拦截：可以基于客户端的运行时环境特征数据实现拦截，包括：客户端指纹，User-Agent 等，实现针对性拦截。
3	动态拦截：当请求触发防护规则时，可以设定多种拦截策略，如：阻挡，延时等；且可配置上述拦截策略按百分比随机响应，提升攻击者的对抗分析难度。
4	客户端环境验证：自动在网页代码中插入 JS 检查代码，JS 代码检查客户端的运行环境，防止恶意终端访问。
5	客户端行为验证：自动在网页代码中插入 JS 检查代码，JS 代码检查客户端的行为，是否存在键盘鼠标行为，从而识别是否是真人操作。
6	客户端指纹：自动在网页代码中插入 JS 检查代码，JS 代码收集客户端环境信息，为每个客户端生成唯一的指纹标识。
7	支持 Ipv6 协议：考虑与现有网络环境的兼容性要求，支持处理 IPv6 或 IPv6/v4 双栈流量。
8	防自动化漏洞扫描：通过对可攻击点的动态隐藏，自动化工具无法获得攻击入口，可有效防止各类已知与未知漏洞的自动化扫描工具。
9	防自动化模拟操作：可防止攻击者通过自动化模拟操作，进行自动化登录操作。
10	防自动化内容搜刮：可防止攻击者通过爬虫或自动化工具，搜刮服务器上的数据或敏感信息。
11	防自动化暴力破解：可防止攻击者通过自动化程序，暴力破解或猜测敏感数据。
12	防重放攻击：可防止攻击者重放先前的交易内容，形成虚假交易或破坏后台数据的完整性。

13	报表功能：支持客户端对网站的全访问记录，可以基于多种维度进行查询，快速生成查询结果。
14	集群和高可用
15	Cookie 令牌
16	自动化工具识别与防护
17	白名单功能
18	日志功能

5.防护域名数量需求

主动防御系统部署后，可以对不少于 90 个域名进行保护。

6.部署场景需求

本次拟部署软件形态产品，结合长宁教育信息中心现有的虚拟化环境，将主动防护系统虚拟机镜像导入虚拟化平台，完成配置后，即可保护网站。

7.虚拟化平台支持

主动防御系统需支持以下虚拟化环境:

1. VMware ESXi 5.1 及以上
2. XEN 4.0 及以上
3. Hyper-V Server 2012
4. Linux KVM

8.虚拟化环境系统性能参考

在以下虚拟化环境的资源下,主动防御系统需到达以下性能:

产品配置	参考配置
虚拟化平台	VMwareESXI
CPU	16vCPU
内存	32GB
硬盘	500GB
性能参数	万兆环境
网络吞吐量	>5Gbps
并发TCP会话数	>450万

每秒新建http请求数	>18000连接/秒
TPS处理性能	>6500

长宁区教育局办公室　　2021年4月21日印发