**山东城市服务技师学院安全运维服务外包项目**

1. **聘请专业的安全运维人员驻场**

提供安全设备的运维和加固服务；针对数据中心的网络架构根据安全评估的风险进行安全域划分和设计；对网络结构进行调整和梳理；对安全设备进行安全策略规划和配置；出现紧急事件后，协助析事件可能的原因，解决各类安全事件；定期提供各类安全报告。

1. **现有现有设备和需要提供的设备要求**

目前，学校已有WAF、IPS设备，为保证网络安全，在服务期间，除使用现有设备外，还需提供必要的网络安全设备，需提供的设备包含：

**1、防火墙设备**

1.1、根据网络实际，将防火墙设备部署在网络安全边界，在实现网络功能的前提下，在防火墙中做最大的安全规则限制。针对相关的应用具体到IP地址（或者地址段）+端口号。从而实现对教育应用的最大化的安全防护；

1.2、为保证学校内部网络免遭僵尸主机的风险威胁，并且能够积极防御木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等威胁攻击，所投设备必需具备独立的热门威胁特征库，同时为保证威胁检出效果其特征库总数需在60万条以上；

1.3、支持业务服务器的自动发现以及业务服务器脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；

1.4、设备需支持蜜罐功能，可以帮助学校定位内网感染僵尸网络病毒的真实主机IP地址，支持对未知域名进行拦截，防止中毒主机访问恶意的域名

1.5、提供不低于以下配置的防火墙设备：网络层吞吐量≥20Gbps，应用层吞吐量≥10Gbps，并发连接数≥500万，新建连接数≥30万CPS，双电源，标准2U机架式设备；配备基础防火墙FW、入侵防御IPS、防病毒AV、僵尸网络检测等功能

**2、日志审计设备**

2.1、提供的日志审计设备旁挂至核心交换机，利用通用的SNMP协议将相关网络设备、服务器设备、存储设备、具体应用以及其他安全设备的日常日志发送至日志审计设备并做好相关保存、记录等工作，根据相关规定保留6个月的日志信息；

2.2、提供的应合理配置使用现有和新增设备，确保网络安全，出现安全威胁后，及时预警并整改，按月出具安全威胁检测和整改报告；

2.3、提供的设备必须支持文本型日志原始文件管理，以便将来数据可以被其他日志服务器使用；

2.4、提供的设备支持内置归并策略，对HTTP数据进行自动归并处理，便于查询

**3、安全运维管理系统**

3.1、支持协议广泛，支持图形协议、传输协议及应用发布功能，

图形协议：RDP、VNC、X11等；字符型协议：SSH、TELNET、RLOGIN、AS400等；

传输协议：FTP、SFTP等；数据库协议：ORACLE、MSSQL、Sybase、Mysql、DB2等；

应用发布：HTTP(S)、VMware、Radmin、Pcanywhere等各种应用程序软件发布，无须软件定制

3.2、提供的安全运维系统采用标准机架式硬件结构，B/S架构，采用HTTPS方式远程安全管理，无需安装管理客户端，保证安全性；

3.3、提供的设备支持运维会话协同操作，以便于运维过程中受管理人员实时监控；

**4、关键服务器系统、WEB应用漏扫服务**

4.1主动发现服务器及Web应用系统中隐藏的漏洞，根据漏扫结果输出详尽的漏洞描述和修补方案。

4.2、服务频次：每月1次，重大政治节点根据甲方要求进行工作。

4.3、服务要求：安全漏洞扫描需包含但不限于以下内容：SQL注入、XSS跨站脚本、伪造跨站点请求（CSRF）、隐藏字段、表单绕过、AJAX注入、弱配置、敏感信息泄漏、HI－JACK攻击、弱口令、Xpath注入、LDAP注入、框架注入、链接注入、操作系统命令注入、Flash源代码泄漏、Flash跨域攻击、Cookie注入、敏感文件、第三方软件、其他各类CGI漏洞支持国际目前主流WEB应用类型。

4.4、服务成果：成交单位每月输出《漏扫扫描报告》并根据漏洞情况提供整改建议。

4.5、服务商须采用专业的扫描工具，兼容CVE、CNCVE、CNVD、CNNVD等数据库，支持IPV6地址。支持漏洞库数量不低于6000条，必须支持虚拟化平台（vmware）漏洞扫描。

4.6、服务商须自有扫描工具，服务期内随时可以被甲方无限次使用。

**三、网络安全管理文档体系建设**

根据等级保护的规定，协助学校进行管理文档、体系、制度方面的工作，建立起符合要求的文档管理体系，包含账号管理流程、配置变更流程、设备管理规定、网络应急预案、外来人员安全管理、培训教育管理等方面的建设，并根据学校的具体需求进行管理文档方面的完善。

**四、安全漏洞处理**

服务商需派专门的技术人员对发现的高危安全漏洞进行处理，保证补丁的及

时更新，并提供补丁管理规范。

**五、网络安全服务能力要求**

1、服务商能力要求

1.1、安全服务商必须与网信、网安部门保持良好的合作，并且有相关合

作的证明；

1.2、安全服务商有专业安全服务资质，满足合规性和规范化操作；

1.3、安全服务商为省信息安全协会认可的服务商，能提供更优质的安全服务，提供相关证明；

2、服务商人员能力要求

2.1、服务商有不少于2名国家认可的CISP安全工程师，配备1人驻场；

2.2、学校的主要安全设备为WAF、IPS设备，服务商要有此产品的相关认证证书；

2.3、服务商有专门的CISAW安全风险管理人员(专业级)，能根据安全安

全隐患作出正确评估；

2.4、服务商有不少于5人以上的二线支持团队。二线支持团队，技术支持团队提供远程技术支持，制定工作流程，监督专业网络安全服务人员的日常管理工作，出现专业网络安全服务人员无法解决的问题时提供远程协助，如果需要现场处理的问题，需要在1小时内到达。

**六 、服务期限：三个月。**