**开平市党群部门网站云防护服务项目采购需求**

1. **项目概述**

**（一）项目背景**

开平市网站集约化后互联网系统及网站有大量互联网网站集约化，互联网系统及网站面临的网络安全风险最高，主要体现在：

1.暴露互联网，最容易遭受反共黑客组织等各类黑客组织攻击；

2.政府类互联网系统及网站，由于其在百度、谷歌、360等搜索引擎排名权重与PR高，很容易被黑产SEO优化团队盯上并利用，植入赌博、色情、暗链、关键词跳转等；

3.党政机关事业单位的系统与网站是各个监管单位重点监管、扫描、安全检测、渗透测试、攻防演练的重要目标，如网信办、公安网监、通管局、市委绩效检查等，也是各类专项行动的重要目标；

4.互联网系统及网站一旦发生安全事件如无法访问、被篡改、存在漏洞，容易被社会公众新闻媒体所知晓，最容易造成社会舆论影响，甚至造成政治影响。

综上所述，采用云防御技术建设并加强开平市党政机关集约化互联网系统及网站的网络安全极其重要，刻不容缓。

目前开平市党政机关集约化互联网系统及网站与内部网络的边界建设了对应的防御体系，具备了一定的攻击防御能力。但是由于外部攻击环境急剧变化，攻击能力的增强如0day攻击、军事武器民用化、钓鱼攻击、跳板攻击、APT定向攻击等可能导致防御系统不能完全防御到位以及攻击与防御能力的不对等。主要的风险点包括门户网站、网上办事大厅、手机办事大厅、暴露的公网IP等一切互联网入口。安全遵循木桶短板原理，只要有一个漏洞或者一个缺陷能够被攻击者利用则安全防护失效。

**（二）项目目标**

采用云防御技术建设和加强互联网系统及网站的网络安全防御能力的主要目标是：

1.满足各类监管要求，解决监管单位发现我市相关系统的漏洞等问题，充分利用替身防御、云防御等技术解决此问题；

2.提升我市场党政机关互联网系统及网站防御能力，防止黑客入侵，保障系统的完整性、可用性、机密性；

3.提供工作效率，降低安全人力资源的投入，解放人力，专注业务，互联网系统及网站安全由专门团队云端集中进行攻防对抗。

1. **服务供应商资格要求**

（一）投报人符合《中华人民共和国政府采购法》相关的规定。

（二）投报人应当是具有合法经营资格的法人，具有良好的信誉；

（三）投报人须有能力提供完善的售后服务，包括：稳定技术人员、响应时间，技术服务人员须有相关工作经验。

（四）本项目不接受联合体投报，不允许转包或分包项目。

1. **项目范围和内容**

1.项目范围

本次利用云防御云防御技术建设和加强互联网系统及网站的网络安全防御能力的范围包括：11个网站系统。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 网站名称 | 网站网址 | 单位性质 |
| 1 | 中共开平市委党校 开平市行政学校网站 | <http://dx.cnkaiping.cn/index.html> | 党群部门 |
| 2 | 开平市红十字会网站 | [http://kphszh.cnkaiping.cn/index.html](http://kphszh.cnkaiping.cn/index.html" \o "http://kphszh.cnkaiping.cn/index.html) | 党群部门 |
| 3 | 开平市妇女联合会网站 | <http://fulian.cnkaiping.cn/index.html> | 党群部门 |
| 4 | 开平市人民代表大会常务委员会网站 | <http://kprdcwh.cnkaiping.cn/index.html> | 党群部门 |
| 5 | 中国共产主义青年团开平市委员会网站 | http://kpqsw.cnkaiping.cn/index.html | 党群部门 |
| 6 | 开平市残疾人联合会网站 | http://clwz.cnkaiping.cn/index.html | 党群部门 |
| 7 | 开平文艺网 | <http://wl.cnkaiping.cn/index.html> | 党群部门 |
| 8 | 开平市纪委监察网 | <http://jiwei.cnkaiping.cn/index.html> | 党群部门 |
| 9 | 中共开平市委机构编制委员会办公室网站 | <http://kpbb.cnkaiping.cn> | 党群部门 |
| 10 | 中国人民政治协商会议开平市委员会网站 | <http://zhengxie.cnkaiping.cn> | 党群部门 |
| 11 | 开平市宣传部网站 | <http://xcb.cnkaiping.cn> | 党群部门 |

2.项目内容

采购云防御SaaS产品，此产品用于项目范围的全部内容大约11个系统，此项目无需部署任何软硬件，为SaaS服务类安全产品，交付账户密码。

1. **Web业务系统安全需求分析**

## 1、业务安全需求分析

综上所述，根据风险分析以及传统WEB解决方案的局限性，web业务系统安全需求如下：

1. 针对WEB业务系统的入侵，数据泄密，被篡改、网络钓鱼、SQL注入和跨站脚本等攻击方式防御能力。
2. 针对WEB业务系统遭受僵尸、木马、蠕虫、病毒等植入的防御能力。
3. 针对WEB业务系统遭受恶意扫描、爬虫等自动化工具获取非授权信息的拦截能力。
4. 针对WEB业务系统的DDoS/CC攻击防御能力。
5. 0day与Nday的防御能力。
6. Web业务系统安全运营的能力。
7. 应对各种监管单位，与监管单位的攻击检查渗透进行对标，使防御能力等于或者高于监管单位的检测渗透扫描能力。

## 2、合规性需求分析

1. 贯彻落实《中华人民共和国网络安全法》；
2. 切合等级保护工作要求。信息系统安全等级保护制度要求对处于第三级保护能力的信息系统开展渗透测试，鉴于WEB业务系统的重要性，可以按照或参考等保要求进行建设，因此利用云防御技术搭建web防护平台切合等级保护的工作要求；
3. 贴近本地信息安全工作要求。开平市对网络信息安全工作历来重视，按照国务院以及市信息安全绩效评估要求，对web业务系统的安全防护报告是其中一项重要工作。
4. **服务技术要求**

|  |  |  |
| --- | --- | --- |
| 产品架构 | 产品形态 | ★基于云、大数据、内容分发等技术为网站安全提供SaaS形式的云防御；非硬件WAF和软件；能够单次反向代理实现CDN、WAF、抗D功能模块，实现同一控制台统一管理功能模块； |
| 防御节点 | ★至少20个分布在各地的防御节点；提供20个以上不同C类网段节点证明；提供增值电信业务经营许可证（内容分发-全国）； |
| 部署方式 | 无需在服务器安装任何客户端，无需要部署任何硬件设备，采用DNS牵引方式进行引流防护，采用NS或者cname方式将网站接入防护，纯SaaS服务方式； |
| 数量 | 数量 | ★提供≧15个系统的业务系统或网站防御； |
| 带宽及性能 | 带宽及性能 | ★对网站及主机的带宽与QPS无限制； |
| 安全防护能力 | 网站防御能力 | ★扫描器/爬虫防御策略，异常HTTP请求防御，SQL注入防护，Webshell防护，XSS防护，命令/代码执行防护，文件包含/注入防护，特殊/其他攻击。（必须提供相关防御能力的管理界面截图证明）； |
| 防扫描 | 具备防恶意扫描，能够对互联网的恶意扫描行为（至少能够识别互联网流行的100款扫描器）进行识别，并将其阻断； |
| 防爬虫 | 具备防爬虫，能够防护针对业务系统的爬取内容和数据（至少能够识别50种类型的爬虫程序）的行为； |
| 入侵防护 | 具备防漏洞攻击，保证高危漏洞出现时在2-6小时内构建安全防护规则，保证门户、业务系统等应用； |
| web防火墙 | 可防护SQL注入、命令注入、跨站脚本、跨站请求伪造、信息探测等攻击； |
| WebShell防护 | 可防止黑客上传、访问WebShell（网站后门）； |
| CC攻击防护扩展能力 | ★提供CC类型拒绝服务攻击防护可扩展能力，以消耗服务器各类资源如CPU、内存、后端数据库的防护能力；提供CC攻击识别方法和设备的发明专利证书； |
| DDOS防护扩展能力 | ★提供可扩展流量型DDOS攻击与CC攻击的防御能力，提供界面截图证明； |
| CDN安全加速扩展能力 | ★提供可扩展CDN能力，包括缓存、页面压缩、协议优化、链接优化等，提供界面截图证明； |
| 内容安全扩展能力 | ★提供可扩展敏感内容识别与拦截能力，将敏感文字、关键字等涉敏信息对互联网展示进行替换。 |
| URL与目录访问控制 | 可以禁止非授权IP访问网站后台管理地址或重要页面； |
| 防盗用 | 保护网站图片、压缩包等资源文件不被其它站点盗用； |
| 适应网站特性能力 | URL白名单 | 可以对特定的URL添加白名单，如接口URL、安全信任URL，至少能够添加50条以上URL； |
| IP地址访问控制 | 可设置不进行防护的IP地址（IP白名单）、不允许访问的IP地址（IP黑名单），各50条以上； |
| 端口适应 | ★支持网站非标准端口（80,443以外端口），自助设置协议和端口，提供管理平台自助设置界面截图； |
| SSL节点支持 | ★对于https类型网站，用户能够自助上传SSL证书到防护平台。（提供管理平台自助上传SSL证书截图证明）； |
| IPV6可扩展能力 | ★无需部署任何软硬件，可扩展支持IPV6与IPV4的转换与防御，将IPV4的WEB系统转换成互联网可解析的IPV6地址与可访问的IPV6 WEB系统；提供截图证明 |
| 安全可视化能力 | 网站访问可视化 | 提供网站访问情况信息展示，包括请求数、总流量、网站浏览人数，搜索引擎引导量，遭受攻击次数等，并能按时间端统计的网站访问量； |
| 受攻击可视化 | 查看网站安全状况，包括各种攻击发生次数，攻击IP、来源（国家）等；可显示对网站的安全评级，如安全、危险等等，可显示历史攻击次数等；可显示CC攻击详细情况；  可显示攻击者的扫描情况，包括时间、攻击URL，攻击者IP及归属地，攻击类型等； |
| 全球地图攻击可视化 | ★提供全球实时攻击视图，在视图中实时显示攻击源IP，国家，目标域名，目标所在地等。（提供管理平台全球地图实时动态防御截图证明）； |
| 统计与分析能力 | 报表 | 支持当日、前一天、最近30天和最近一年的报表统计下载 |
| 日志 | 提供最近7天内的攻击和访问日志自助下载服务； |
| 安全防护成熟度 | 案例证明 | ★提供至少四个部委级或者国家级官方门户网站的防御证明，提供域名解析的截图证明。 |
| 合规性资质 | 产品资质 | ★公安部销售许可证，必须是云防御类；提供销售许可证证明。 |
| ★信息系统安全等级保护备案证明，必须是三级或以上的云防御类系统；提供公安机关备案证明； |
| ★增值电信业务经营许可证：全国内容分发网络业务 |
| ★可信云：云分发服务 |
| ★公安部云计算产品信息安全认证证书，必须是云防御类产品。 |
| ★CSA云安全联盟证书。 |
| ★厂商资质 | 国家信息安全测评中心的信息安全服务资质证书（安全工程类）。 |
| 国家信息安全测评中心的信息安全服务资质证书（风险评估）。 |
| 中国网络安全审查技术与认证中心的信息安全服务资质（应急处理）。 |
| 中国网络安全审查技术与认证中心的信息安全服务资质（安全集成）。 |
| 中国网络安全审查技术与认证中心的信息安全服务资质（安全运维）。 |
| ISO/IEC 20000标准的信息技术服务管理体系认证。 |
| ISO/IEC 27001标准的信息安全管理体系认证。 |
| ISO 14001标准的环境管理体系认证（覆盖计算机软件相关环境管理）。 |
| ISO 9001标准的质量管理体系认证(覆盖计算机软件相关质量）。 |

1. **项目功能**

|  |  |  |
| --- | --- | --- |
| 名称 | 功能 | 备注 |
| 网站安全云防御 | 提供域名专业版云防护服务，含11个域名云防御；包含以下内容：智能DNS; web防火墙；防火墙策略集控制；防护策略屏蔽时间；防火墙策略白名单；智能攻击防御；webshell防护；后台锁（10条）；防盗链（10条）；整站设置；可视化；攻击预警；数据下载；一键关停；日志审计；ssl证书；清洁流量（12TB/主域名.年);防火墙兼容性测试；重保标准支持；7x24小时电话支持服务、产品咨询以及问题远程支持。 | 一年云防御服务 |

1. **服务报价**

本维护项目最高限价为人民币165000元，投报报价不得超过最高限价。

1. **确定成交供应商**

若有多家供应商竞价，采购人将综合考虑供应商的服务质量、技术服务能力、采购信誉度、与本单位有服务经验者等方面进行择优选择，确定为成交供应商。

1. **服务期限及结算方式：**

服务期限为1年，结算方式：按合同约定方式结算。