**宁波城市职业技术学院校园网络信息安全服务项目需求**

**一、项目服务内容要求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务类别** | **服务名称** | **服务内容** | **服务周期** |
| 1 | 安全运维服务 | 网站及业务系统安全监测服务 | 1远程网页木马监测2.网页敏感内容监测3.网页篡改监测4.服务质量监测5.其他风险监测能力 | 7\*24小时 |
| 2 | 信息系统漏洞扫描及安全加固服务 | 每月提供现场的脆弱性扫描评估，针对应用系统、操作系统、网络环境进行扫描，并对扫描服务发现的漏洞进行梳理分析，要求能够提供专业有效的解决建议，同时并能够配合进行整改，直至漏洞完成修复。 | 每月一次 |
| 3 | 安全巡检服务 | 每月对信息系统中包括网络设备、主机设备、安全设备进行一次全面地安全巡检，主要内容包括漏洞审查、策略检查、日志审计等，如有异常情况，及时与项目接口人沟通，提供安全咨询的建议。 | 每月一次 |
| 4 | 安全报表服务 | 每月将监测、巡检、扫描结果分析和形成的评估结论，汇总信息安全报告，并根据现状与要求之间的差距，分析系统存在的问题，提出改进建议。 | 每月一次 |
| 5 | 安全评估服务 | 信息系统资产详细调研服务 | 本项目要求在项目服务初期，对项目涉及的信息系统资产进行一次详细梳理，形成《信息系统信息汇总表》。信息系统调研信息汇总表作为其他服务项目的参考资料，应包括信息系统名称、IP地址、主机操作系统、数据库软件、网络设备固件、开发/维保联系人等信息。 | 每年一次 |
| 6 | 信息系统安全配置核查 | 本项目要求对项目涉及的信息系统设备每年进行一次安全配置核查，针对网络设备、专用安全设备、服务器操作系统、数据库系统等，通过人工核查及工具核查相结合的方式，发现因策略配置不当导致的安全脆弱性。安全配置核查完毕后，应形成安全配置核查报告。 | 每年一次 |
| 7 | 整体风险评估服务 | 在本项目服务期限内，对全网信息系统进行整体风险评估。整体风险评估，应对浙江学院全网存在的问题作详细分析，并给出解决方案。在项目服务后期，形成风险评估报告。 | 每年一次 |
| 8 | 信息系统变更及上新安全评估服务 | 本项目服务期限内，要求对浙江工商职业技术学院所有变更后的信息系统以及新上线的信息系统进行安全评估。确保信息系统变更不会引进新的安全风险，确保新上线的信息系统不带病上线。 | 全年 |
| 9 | 高级威胁分析服务 | 在本项目服务期限内，定期在学校部署APT分析平台，对城市学院存在的重要安全问题作详细分析，并给出解决方案。 | 每月一次 |
| 10 | 安全咨询/技术保障服务 | 重大活动技术支持 | 在重大活动、节假日期间提供必要的技术支持和人员支持，按需求提供安全保障。包括重要系统巡查、安全加固等等。 | 全年 |
| 11 | 应急响应支持 | 在本项目服务期限内，提供7×24 小时应急响应技术支持电话，在出现突发安全事故时提供及时的应急支持，接到应急响应请求时迅速启动响应预案； | 全年 |
| 12 | 安全培训服务 | 安全运维服务期限内提供一次安全培训，培训内容包含：安全意识培训、产品使用培训，安全管理培训，安全技术培训，攻防实践演练培训，应急响应实践演练培训等。 | 每年一次 |
| 13 | 政策合规管理服务 | 在招标人现行安全管理制度基础上，依据国家相关标准（如信息系统安全等级保护标准、及信息安全管理体系标准），协助招标人进行安全管理制度的梳理和建设，建立健全网络层、系统层、应用层、以及数据层的安全管理制度及规范，并且建立起覆盖信息系统开发和运维生命周期的管理规范，如面向信息系统开发的安全编码规范，以及面向信息系统运维事件的应急响应规范（含应急处置预案）。 | 全年 |
| 14 | 安全咨询服务 | 安全咨询服务应当包括管理咨询服务和技术咨询服务，投标方应承诺，针对招标人在服务周期内产生的与信息安全技术有关的咨询需求，提供专业的咨询意见。安全技术咨询的范围包括计算机网络、网络安全设备、服务器主机系统、数据库与中间件、应用系统等。 | 全年 |

1. **玄武盾云防护一年服务**

在本项目服务期限内，在学校部署玄武盾云防护服务，对城市学院主域名进行防护。

|  |  |
| --- | --- |
| **指标项** | **玄武盾指标要求** |
| 域名 | nbcc.cn，nbcc.edu.cn |
| 平台要求 | \*全国范围内具备至少20个云防护和CDN加速节点，并提供证明 |
| \*要求安全防御平台为一体化平台，应同时具备网站漏洞监测、安全事件监测、可用性监测、攻击防御状态、防护报表等功能,要求所有的功能集成在同一产品上实现。所要求的功能需要提供截图 |
| 能为每个网站用户单独创建用户账号，用于查看网站和系统的安全状况。监管用户可关注、查看所有下属机构的网站和系统整体情况。 |
| 近三年内原厂商具有9个不低于50万元的云防护服务合同，并提供合同复印件 |
| 部署方式 | 无需在网站前端安装任何安全设备、软件，通过DNS别名指向到云端进行安全防护 |
| 防御功能 | \*能提供不低于2Tbps的DDOS流量清洗能力，并提供证明文件； |
| 支持DDOS防护算法调整，如可选择至少三种SYN Flood攻击防护机制，可自定义设置流量、连接数等触发防护阀值； |
| 连接型DDoS攻击防护，过滤TCP慢速连接攻击、连接耗尽攻击、tcp新建连接限制等攻击和loic、hoic、slowloris、Pyloris、xoic等慢速攻击 |
| 系统应具有常用应用层协议（如HTTP、FTP、GAME、DNS等）防护插件； |
| 特征过滤，4层ip+port过滤和7层payload部分内容过滤 |
| 支持检查提交的报文是否符合HTTP协议框架，如异常的请求方法、特殊字符、重点字段的缺失、超长报文造成的溢出攻击以及对高危文件的访问等 |
| 支持识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括SQL注入、命令注入 、Cookie 注入等）、跨站请求伪造等应用攻击行为 |
| 支持识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷 |
| 支持基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力 |
| 支持对用户上传的文件后缀名和文件内容进行全方面检查，杜绝Webshell的上传和访问 |
| 支持对WEB服务器容器、应用中间件、CMS系统等第三方组件漏洞进行有效防护 |
| 支持区域访问控制，限制国外用户或者国内以省市为单位的区域进行访问控制。 |
| 支持智能识别攻击者，对网站连接发起攻击的IP地址进行自动锁定禁止访问被攻击的网站。 |
| \*支持协同防护，平台够整体联动，对攻击IP进行全面封锁。 |
| \*支持一键虚拟补丁功能，网站出现0day漏洞时能快速完成修复，提供界面截图并加盖公司公章。 |
| \*支持永久在线功能，当网站因为服务器故障、线路故障、电源等问题出现无法连接时，可显示云防护节点中的缓存页面。当在敏感期或特殊时期时，用户网站主动关闭期间可显示缓存页面，增强网站安全性。提供界面截图并加盖公司公章 |
| \*支持一键关停功能，当网站出现紧急安全事件时，可在一分钟内通过手机APP和浏览器一键完成关停，防止产生恶劣影响，提供界面截图 |
| \*网站防篡改 | \*提供防篡改软件（与云防护同一品牌），采用先进内核驱动和实时触发技术，内核自定义编译，支持各类网页文件的保护，禁止非法文件篡改，包括静态和动态网页以及各类文件信息，提供公安部销售许可证、国家保密局涉密信息系统安全保密检测中心检测证书、中国信息安全测评认证中心颁发的中国国家信息安全产品认证证书（提供加盖公章的证明文件）。 |
| \*网站监测服务 | 提供事前漏洞扫描服务，对网站存在的脆弱性进行探查，包括SQL注入漏洞、跨站脚本漏洞、开放服务漏洞、网站第三方应用漏洞0day漏洞等； 具有大规模漏洞扫描能力，每日扫描网站最多可达一万个（提供证明材料并加盖公章） |
| 提供漏洞自动跟踪服务，服务的依托的产品可以自动对检测到的漏洞进行跟踪，督促问题网站进行整改。 |
| 提供事后安全事件监测服务，监测内容如下：  1、对网站被植入暗链进行监测，包括对广告、游戏、博彩、色情、医疗、推广等类型的暗链进行监测。 （已检测到的暗链URL不少于150万个，提供截图证明） 2、对网站黑页进行监测； 3、对网站篡改变更进行监测； 4、对网页敏感内容进行监测，如“博彩”、“色情”等； 5、对网站坏链、无效链接、错链进行监测； 6、对反共黑客事件进行7\*24小时的专人值守监测； （敏感关键字策略数不少于2万个，并提供截图证明） |
| 提供可用性监测服务，可对用户网站进行全国多节点的监测，监测发下可用性性异常情况： 1、监测网站服务是否中断或报错 2、监测网站延时是否过大 3、通过多线路监测是否存在线路异常 实时通过全国至少20个节点，对网站服务质量进行监测能监测网站的打开时间，资源加速速度等多个维度的质量 （提供节点的证明文件和多节点可用性监测的监测截图并加盖公章） |
| 安全审计 | 提供访问日志记录与查询功能，可根据域名、URL、客户端IP、返回码、访问区域、访问时间段进行查询，查询后的日志数据可导出Excel文件。 |
| \*提供攻击日志记录与查询功能，攻击日志至少保存6个月，满足《网络安全法要求》，可根据域名、URL、攻击方法、返回码、威胁等级、攻击IP、攻击区域和攻击类型进行查询，查询后的攻击日志数据可导出Excel文件。 |
| \*提供访问与攻击原始日志离线下载功能，可按天进行下载，原始日志包含访问IP、访问时间、URL、返回码、UA、访问域名等信息。 |
| 报表 | 可查看安全防护报告，包含攻击流量、攻击者区域统计、攻击者IP统计、被攻击页面统计、被攻击域名统计、攻击事件统计、攻击威胁等级统计等报告。 |
| 可查看网站访问报告，包含访问流量、访问区域统计、访问源IP统计、访问页面排行、访问终端、死链、静态资源等统计报告 |
| 可查看服务质量监测报告，包含全国各省监测节点可用性分析、线路故障、CDN命中分析、首页加载时长分析、网站更新频率分析等 |
| 支持日报、月报 ，并支持html、pdf格式导出。 |
| 支持单个网站生成报表，也支持网站群生成一个汇总报表 |
| 可视化展现 | 可视化页面需要可以投放到大屏幕，分辨率不低于1400\*900； |
| 整体网站群攻击态势可视化分析，包括访问与攻击流量趋势、CC攻击趋势、受攻击网站趋势、攻击IP排行、网站访问排行等、攻击区域热点展示与挖掘 |
| 单个网站可视化分析，包括访问流量、访问区域热点展示、访问与攻击源实时分析、访问源IP排行、攻击趋势、攻击区域分布、攻击类型、攻击时段、攻击源IP排行等数据展示与挖掘 |
| 手机APP管理 | \*通过手机APP查看网站整体防护态势，包含网站漏洞监测、可用性监测、攻击防御状态、防护报表、页面防篡改等状态信息，提供现场演示 |
| \*通过手机APP完成防护配置，包括一键关停、防护模式、永久在线等功能。 |
| 服务告警方式 | 根据不同告警级别发送邮件、短信、电话等多种告警方式 |
| 服务能力 | 本次项目的服务人员需要有面向CN/CERT、公安部提供安全通报服务的经验，并在近三年内获得公安行业通报工作的相关奖励；（提供至少2份获奖证明）。 |
| \*具有7\*24小时反共黑客值守及应急响应能力，提供反共事件发现截图及分析报告证明 |
| 本次安全厂商需要向公安部、20个以上的cert分中心以及各地的公安部门提供安全通告经验，至少有通告3000多起事件。 |
| \*具有云端7\*24远程安全专家服务能力，提供7\*24小时安全值守和应急响应服务。提供策略优化、配置调整、规则更新、问题处理、技术咨询安全事件通告等常规技术支持服务，实时监测和感知DDOS、持续性攻击、0day攻击等事件，并及时响应和对抗，同时在重大节会期间提供更高级别的安全响应服务，需提供相关的证明材料（含办工场地，人员情况，服务过程性材料截图等）。 |
| \*具有G20峰会、世界互联网大会、上合组织峰会、一带一路等国际峰会官网云防护安保案例，提供官方感谢信或证明文件 |

1. **资质及服务团队要求**

**本次项目包含安全运维服务类项目，特别注重投标人自身安全服务能力以及所能涉及的服务范围，因此对投标人技术水平要求较高，需要投标人满足以下企业资质及人员资质要求。**

（一）投标公司应是在信息安全领域须具有丰富的经验和先进的技术，能满足以下资质要求之一：

1、投标人应具有中国信息安全认证中心颁发的信息系统安全运维二级及以上服务资质证书；

2、投标人应具有有效的计算机信息系统集成叁级及以上资质。

（二）投标人提供业绩证明。

**具体要求：**

投标人自2015年1月1日以来承担过宁波市高校行业大规模信息安全运维服务供应及实施工作。需提供至少5个项目案例，每个案例的合同金额不少于15万元。

上述案例材料中须包括项目名称、最终用户的有效联系方式、项目金额等，并提供与用户签订的合同首页、标的及其金额所在页、签字盖章页及产品明细清单的复印件等确切的相关资料。

（四）服务团队要求

**具体要求：**

投标商必须提供维护实施组人员名单（6人以上）；其中项目经理必须具有CISP认证资质；运维实施人员至少一名H3C、华为或CISCO认证工程师；以上人员提供资质证书复印件并加盖公章，并提供近3个月社保证明。