**信息系统安全服务**

1. 服务简介

1）服务范围

对宁波市市场监督管理局保税区 （出口加工区）分局的应用系统进行安全扫描评估，其评估范围包括漏洞扫描（主机、应用）、服务器后门及木马扫描、对主机方面漏洞提供安全加固建议、协助业主单位建立、完善信息安全管理制度（包括应急响应等管理制度）、风险评估、安全巡检、互联网应用安全监测、应急响应等。

2）服务期限

服务周期为一年。

二、技术服务内容

| 服务类型 | 服务子项 | 服务说明 | 服务级别 |
| --- | --- | --- | --- |
| 测试评估服务 | 技术评估服务 | 根据信息系统安全特性，从技术层面评估系统整体的安全性，发现系统风险的同时提出合理的风险管控方案。 | 每年一次 |
| 漏洞扫描服务 | 主机漏洞扫描 | 使用专业的主机漏洞检测工具，对主机系统的安全脆弱性进行检测，从而发现潜在的安全问题和系统漏洞。 | 每季一次 |
| WEB漏洞扫描 | 使用专业的WEB漏洞检测工具，对WEB系统的安全脆弱性进行检测，从而发现潜在的安全问题和系统漏洞。 | 每季一次 |
| 优化加固建议 | 根据信息安全标准，建立专属《安全基线》，提供配置加固、策略调整、补丁安装等安全加固建议。 | 全服务期 |
| 应急保障服务 | 应急响应服务 | 提供5\*8小时的远程技术支持和7\*24小时的紧急现场救援，15分钟远程响应，必要时2小时内赶到客户现场。 | 7\*24 |
| 应急预案修订 | 根据信息系统的实际需求，结合当前系统的网络环境及政策法规要求，协助客户制定或修订应急预案。 | 每年一次 |
| 其他安全服务 | 安全迎检服务 | 解读各种网络安全政策、法规及标准，协助客户完成来自监管、主管部门的各项信息安全咨询管理工作。 | 全服务期 |

三、技术服务内容要求

1、测试评估服务

1）技术评估服务

投标人须提供技术评估服务，梳理并建立资产库，根据目标系统的安全特性，依据国家相关安全标准，从技术层面评估系统安全脆弱性，识别系统安全风险的同时提出合理的整改加固建议，并协助采购人落实整改加固措施，输出技术评估报告。

2、运行维护服务

1）主机漏洞检测

投标人须提供主机漏洞检测，使用专业主机系统漏洞检测工具，基于漏洞扫描技术，定期对指定目标主机的安全脆弱性进行检测，发现目标主机依存的安全漏洞，并给出专业的修复建议且尽可能的协助落实修复措施，输出主机漏洞检测报告。

2）web漏洞检测

投标人须提供互联网web漏洞检测，使用专业WEB漏洞检测工具，基于漏洞扫描技术，定期对指定WEB系统的安全脆弱性进行检测，发现并验证目标系统依存的安全漏洞，并给出专业的修复建议且尽可能的协助落实修复措施，输出web漏洞检测报告。

3）优化加固服务

投标人须提供优化加固的建议，根据信息安全相关标准及政策法规要求，建立信息系统专属《安全基线规范》，并采用配置加固、策略优化、补丁修复等方式，协助采购人实施对目标系统的安全加固。

4、应急保障服务

1）应急响应服务

投标人须提供应急响应服务，依靠多年的安全攻防技术和应急处理经验积累，参照国家信息安全事件响应处理相关标准规范，帮助采购人在发生安全事件后，按照标准应急响应流程，提供7×24全年无休的应急响应服务。

2）预案编制服务

投标人须提供预案编制服务，依据《网络安全法》、网络安全等级保护2.0相关标准要求，在全面了解采购人安全管理现状、业务流程、组织架构等基本信息的基础上，协助采购人编制或完善信息安全应急预案。

5、安全咨询服务

1）安全迎检服务

投标人须提供安全迎检服务，协助采购人深层次解读各种网络安全政策、法规及标准，帮助采购人做好网络安全风险管理与规避，更好的应对监管部门日渐常态化的各项网络安全及合规检查，协助采购人顺利完成相关安全工作。

四、服务要求

服务人员需要严格按照采购人要求的相关安全服务规范开展工作，包括制定服务计划、编写方案、执行安全评估并提交相关报告、协助安全加固等，具体要求如下：

1. 投标单位需自行到现场进行勘察，以确保对服务对象、服务范围以及工作量的准确评估，在投标文件中提交符合业主单位需求的服务方案，提交现场勘查证明函并加盖业主单位公章；投标单位应于2020年11月3日上午10:30到宁波市北仑区保税区兴业大道2号楼4楼市场监督管理局B444办公室进行项目现场踏勘，过时不候，未参与现场踏勘的供应商，不具备中标资格。
2. 要求提供详细的安全服务技术方案，方案中应包含对服务对象的详细调研报告，包括应用系统清单、主机操作系统情况、应用系统基本功能以及详细的网络IP情况等。项目实施方案中要体现各项服务内容实施方法、服务工具及人员配置、风险控制方案、项目进度安排、服务成果输出等。
3. 要求规范提供检测报告、事件报告及其他相关服务报告，方案中须明确各阶段交付的报告清单、报告模板。

3、本项目要求提供对服务工具的详细说明，服务工具要求如下：

（1）主机漏洞扫描器：必须提供主流品牌扫描器，用于主机漏洞检测；

（2）应用漏洞扫描器：必须提供主流品牌扫描器，用于应用漏洞检测；

4、针对应急响应服务，要求提供详细的应急响应服务机制，包括事件定级、应急响应时间及应急流程等。

5、服务方及人员须对本次安全服务项目实施过程的数据和结果数据严格保密、未经授权，不得泄露给任何其他单位和个人，同时应在项目结束之后销毁所有和本项目相关的数据和文档。

6、合同签定后，因中标人服务响应不及时或服务内容、工具、人员不符合采购要求，经采购方提醒后仍拒不整改，采购方有权终止合同，且不支付任何款项。

7、因中标人原因造成信息安全责任事故产生重大损失或不良影响的，采购方有权随时终止合同，不支付任何合同款并保留追偿权。

8、本项目不允许分包或转包。

9、本次投标金额不得高于30000元整。