附件4

**服务内容承诺书**

本单位对招标内容及要求中的服务范围和服务期限知晓并同意。本承诺书与招标单位发布的《服务内容承诺书》一致，仅对偏离内容进行补充。

|  |  |  |  |
| --- | --- | --- | --- |
| **服务内容** | **详细要求** | **要求** | **偏离内容** |
| **3.1安全检测服务** |  | 每季度开展1次安全检测服务，全年4次，工程师到现场进行安全运维，运维内容包括网络安全检测、主机安全检测、内网终端检测、信息系统的漏洞检测、数据库安全检测，漏洞补丁升级。所有检测项目在检测后提供详细的检测评估报告,包括电子档材料。 |  |
|  | 3.1.1主机安全检测 | 1、检测防病毒系统运行状况。主要检查主机是否安装防病毒系统，病毒库是否为及时更新升级，是否定期查杀病毒等。2、检测主机授权管理和访问控制状况。主要检查主机是否制定详细的授权管理和访问控制策略，限制不必要权限，口令的复杂度及锁定策略等，是否存在多余默认账号和弱口令。 |  |
|  | 3.1.2网络安全检测 | 1、梳理网络拓扑与设备清单。主要检查网络拓扑设计的合理性，是否符合相关规定要求以及设备清单等信息资料是否准确完整等。2、检测网络设备运行状况。主要检查交换机、路由器等网络设备是否运行良好，同时对网络设备的日志进行分析。3、检测安全防护措施运行状况。主要检查防火墙、入侵防御、数据库审计、堡垒机等设备的运行情况，确保上述设备正常运行，病毒规则库的及时更新，配置策略的优化，对安全日志进行分析。4、检测主机性能状况。主要检查主机运行的服务是否遵循最小化原则，关闭不必要的服务，降低业务风险。5、检测补丁更新状况。主要检查操作系统补丁是否及时更新，是否存在安全漏洞，安装软件是否存在漏洞，并进行补丁升级。 |  |
|  | 3.1.3内网终端检测 | 1、内网终端系统安全风险扫描。扫描终端是否存在安全漏洞、危险应用以及不必要的服务，安全策略的配置是否存在风险。2、终端恶意代码扫描。查杀恶意软件、恶意代码。 |  |
| 3.1.4信息系统的漏洞检测 | 检测源代码危险函数使用、系统中身份认证安全、会话管理安全、上传下载、信息泄漏、数据验证等方面，评估系统在信息泄漏、数据破坏、身份仿冒等方面的安全风险。 |  |
| **3.2网站安全监控及风险预警服务** | 3.2.1监测服务 | 服务周期内全年对门户网站开展监测服务。每隔5分钟进行网站可用性监控、域名劫持监控，每周1次网页挂马分析、暗链分析、敏感内容识别。发现问题1小时内，通过邮箱或电话发出警告，并及时提供发现问题的定位点。当互联网爆发严重安全漏洞或重大安全事件时，及时通知用户并给出初步的风险排查和防控建议，最大程度减轻或避免用户受到安全漏洞或安全事件的影响，提供详细的事件或者漏洞说明，内容包括问题复现方法、解决修复方案和修复验证方法。 |  |
| **3.3应急保障及技术支持服务** | 3.3.1应急保障 | 提供全年应急保障，当发生安全事件时，可根据用户需要，安排安全工程师上门响应，工作时间30分钟内响应，2小时内到达现场（市内），非工作时间1小时响应，4小时内到达现场。提供信息安全技术支撑，协助用户快速定位问题，减轻或消除事件影响，同时协助进行事件取证并提供后续的防控建议和措施。 |  |
|  | 3.3.2其他技术支持 | 其他技术支持内容包括，针对不少于5个指定信息系统的安全漏洞扫描，括sql注入、xss注入、恶意文件上传、命令执行等。全年5次提供Linux系统及windows系统服务器的补丁升级服务。（其他技术服务范围不仅限于门户网站） |  |
| **3.4安全应急预案修订及演练服务** |  | 针对门户网站的实际情况，协助对门户网站的安全应急预案进行实时的修订调整，并针对应急预案开展一次安全应急演练，演练内容包括制定演练方案，提供相关技术人员，提供完整的应急演练报告。 |  |
| **3.5安全培训服务** |  | 每年提供1次派遣资深专业的安全服务工程师到现场进行安全培训服务。培训内容包括网络安全法律法规、网络安全意识培训、最新的网络安全技能培训。 |  |