附件

# **福建省国防动员办公室2024-2026年度**

# **网络安全保障服务内容及要求**

一、服务期限

服务期限为自合同签订生效之日起2年。

二、服务范围

服务范围1：福建省国防动员办公室政府网站

服务范围2：福建省支前动员工作指挥系统、手机安全通信系统、财务预算综合管理平台

服务范围3：安全产品维保服务

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备类型 | 设备型号 | 购买日期 |
| 1 | 安全网关  （互联网、政务外网） | 黑盾安全网关  V4.0/HD-SGS-N1-1616-9 | 2017/8/22 |
| 2 | 防火墙  （政务信息网） | 黑盾防火墙  V3.5/HD-FW-1616-9 | 2017/8/22 |

三、供应商服务资质要求

供应商应具备与本项目服务内容相关的网络安全服务资质。

四、服务内容及要求

| **序号** | **服务类别** | **服务范围** | **服务项目** | **服务主要内容** | **交付成果** | **服务**  **频次** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 安全测试类服务 | 服务范围1 | 网站安全检测服务 | web漏洞扫描服务：采用自动化检测工具与平台全面检测Web应用程序的安全性，深度挖掘程序中存在的各种漏洞和所面临的威胁。 | 定期对服务范围内的网站系统进行安全检测，并提交《网站安全检测报告》 | 2次/年 |
| 2 | 漏洞深度测试服务：通过使用漏洞挖掘工具和检测平台，来测试和识别Web应用系统当前的安全漏洞和存在的安全脆弱性，全面了解和掌控Web应用系统的安全状况。 |
| 3 | 漏洞人工验证服务：对发现的安全漏洞进行人工验证。 |
| 4 | 服务范围2 | 业务系统安全检测服务 | 漏洞扫描服务：采用自动化检测工具与平台全面检测业务系统的安全性，深度挖掘程序中存在的各种漏洞和所面临的威胁。 | 定期对服务范围内的业务系统进行安全检测，并提交《业务系统安全检测报告》 | 2次/年 |
| 5 | 漏洞深度测试服务：通过使用漏洞挖掘工具和检测平台，来测试和识别业务系统当前的安全漏洞和存在的安全脆弱性，全面了解和掌控业务系统的安全状况。 |
| 6 | 漏洞人工验证服务：对发现的安全漏洞进行人工验证。 |
| 7 | 服务范围1及服务范围2 | 渗透测试服务 | 模拟黑客对目标系统进行渗透攻击，深度挖掘目标系统的漏洞与脆弱性，覆盖所有应用功能模块。 | 定期对服务范围内的目标系统进行渗透测试，并提交《渗透测试服务报告》 | 1次/年 |
| 8 | 入侵防护类服务 | 服务范围1 | 网站服务器入侵清查服务 | 网页木马查杀：针对网站源代码进行Webshell查杀，深入检查包括上传图片、文本、脚本以及其他可疑的网站后门程序。 | 服务器入侵清查服务完提交《网站服务器入侵清查报告》 | 2次/年 |
| 9 | 系统后门检查：网站被入侵潜伏后，通常存在隐藏比较深的系统后门（Rootkit），重点发现绕过杀毒软件的系统后门。 |
| 10 | 入侵痕迹检查：针对主机账号、启动项、进程、网络连接等进行检查。日志分析服务：根据系统层日志、安全日志、应用层日志以及其他特征发现网站入侵痕迹，避免黑客使用隐藏账户等躲避检查的安全隐患。 |
| 11 | 安全加固类服务 | 服务范围1及服务范围2 | 服务器系统加固 | 通过对系统层漏洞检测结果的分析，对在检测中发现的系统安全问题提供安全加固建议，提高系统的整体安全性能。 | 定期对服务范围内的目标系统进行安全加固服务，并提交《安全加固报告》 | 2次/年 |
| 12 | Web服务器（中间件）加固辅导 | 针对Apache/IIS/Tomcat等Web应用服务器（中间件）进行配置加固辅导。 |
| 13 | 数据库安全加固建议 | 最大程度降低数据库系统（SQL Server，Oracle等）本身的漏洞风险及加强数据库系统账号、密钥、权限等带有安全风险的配置，从而从整体上提升数据库系统的安全性。 |
| 14 | Web源代码审查及加固辅导 | 发现网站存在高危漏洞，及时采取可行的源代码加固措施，协助开发商进行源代码加固。首次安全加固后，进行漏洞复查和对比，形成加固前后对比。 |
| 15 | 安全监控类服务 | 服务范围1 | 网站安全监控服务 | 网站可用性监控服务：全年每隔5分钟一次对网站首页进行轮询探测，网站访问不到则进行告警，确保网站的可用性、安全性。 | 全年通过专业的网站安全监控平台对网站进行安全监控服务并提交《安全监控报告》4份/年 | 全年 |
| 16 | 域名劫持监控服务：全年每隔5分钟一次对网站首页进行域名劫持探测，一旦发现域名被劫持则进行告警。 |
| 17 | 网页挂马监控服务：每周一次采用远程监控方式对网站页面进行网页挂马分析，一旦识别到网页挂马行为，则进行告警。 |
| 18 | 网站暗链监控服务：每周一次采用远程监控方式对网站页面进行暗链分析，一旦识别到网页存在暗链行为，则进行告警。 |
| 19 | 敏感内容监控服务：每周一次对关键网页的敏感内容进行监控，识别网站存在政治、低俗等敏感内容情况，并告警。 采用的安全服务工具能够发现网页木马(webshell)，须同时支持对反动、赌博、色情等内容进行检查。检查的目标文件类型不限，可同时支持PHP、ASP、JSP、ASPX、JSPX等脚本类型；支持对各类威胁进行自动评分，并按照危险值从高到低进行排序；支持导出检测结果，支持对可疑文件进行批量复制或批量删除。 |
| 20 | 网站监控人工告警服务：针对网站监控平台发现的问题，监控平台发送告警信息到监控值班人员的手机，由值班人员进行人工验证，确认为安全事件后，进行人工电话告警。 |
| 21 | 网站安全监控报告：定期汇总安全监控情况，并提交详细的监控报告。 |
| 22 | 安全巡检类服务 | 服务范围1 | 远程安全巡检服务 | 网站应用层的安全检测与安全加固辅导；对web应用进行远程漏洞扫描，测试web应用安全漏洞问题，并对发现漏洞进行人工验证服务。 | 定期派遣专业技术人员在远程对目标信息系统进行安全巡检服务，针对远程安全巡检发现的问题提出加固建议和辅导服务，并提交《网站远程安全巡检报告》。 | 4次/年 |
| 23 | 中间件安全检测与安全优化建议；针对Apache/IIS/Tomcat等Web应用服务器（中间件）进行配置加固辅导与优化。 |
| 24 | 数据库安全检测与安全加固建议；对数据库服务器进行安全配置核查，对数据库帐号、权限、配置、审计等方面进行核查，及早发现数据库系统存在的风险，并提供安全优化建议。 |
| 25 | 登录网站后台进行漏洞检测与安全加固辅导，并提供加固建议。 |
| 26 | 安全保障类服务 | 服务范围1及服务范围2 | 远程安全咨询服务 | 发生故障时采购人能立即以电话咨询或远程维护方式与供应商取得联系，供应商应立即给予技术协助，提供7×24小时服务支持。 | 安全咨询 | 全年 |
| 27 | 现场应急响应服务 | 当单位网络和信息系统遇到黑客攻击或网页篡改等恶性事件，并且远程支持无法解决时，要求2小时内到达现场，实施最有效的紧急救援及恢复补救方案。 | 发生安全事件时提交《应急响应报告》 | 全年 |
| 28 | 安全通告服务 | 提供最新的安全动态、技术和安全信息，包括实时安全漏洞通知、定期安全通告汇总和安全知识库更新等。通告内容包括但不限于以下内容： 国内外最新重大漏洞、病毒安全通告； 国家安全政策及法律法规； 同行业安全威胁事件通告； 国内外重大安全事件，新技术发展动态通告； 重大安全漏洞爆发时需结合 资产情况，提出相应修复建议。 | 一年不少于6期提交《安全通告》 | 全年 |
| 29 | 服务范围1及服务范围2 | 安全检查专题服务 | 安全检查协助：在上级监管部门安全检查期间，应按要求进行专门的全面安全检查协助服务和保障协助。 | 安全检测报告 | 按需提供 |
| 30 | 管理制度辅助建设：协助制定信息安全管理制度。 | 安全检查相关制度 | 1次/年 |
| 31 | 应急演练 | 应急演练服务 | 网络与信息安全应急预案：定制5个预案场景的《安全应急预案》 | 《安全应急预案》 | 1次/年 |
| 32 | 网络与信息安全模拟应急演练：针对1个预案场景进行模拟应急演练，并提交《安全应急演练报告》 | 《安全应急演练报告》 | 1次/年 |
| 33 | 安全培训类服务 | 单位指定人员 | 安全意识培训服务 | 安全意识现场培训服务：由安全服务工程师提供现场培训服务，培训内容包含但不限于以下方面：安全标准、政策法规解读，信息安全意识、信息安全发展方向，周期性安全服务报告解读，可定制培训内容，一次培训时长1个课时（45分钟） | 安全培训相关材料 | 1次/年 |
| 34 | 安全技术培训服务 | 安全技术现场培训服务：由安全服务工程师提供现场培训服务，培训内容包含但不限于以下方面：网站安全防护、等保安全建设、网络安全技术攻防、无线网络安全防护等，可定制培训内容，一次培训时长1个课时（45分钟） | 安全培训相关材料 | 1次/年 |
| 35 | 安全产品维保服务 | 服务范围3 | 远程支持服务 | 在服务期内，针对维保范围的产品提供远程支持服务。产品出现故障，采购人可通过电话方式，将故障情况报告给供应商。供应商工程师将对采购人提出的问题进行诊断解决。如不能通过电话解决，工程师将通过远程联机方式解决故障。 | -- | 按需提供 |
| 36 | 现场支持服务 | 在服务期内，针对维保范围的产品提供现场支持服务。根据问题，通过电话交流或者远程调试无法解决的，供应商应在2小时内响应并到现场维护。 | 《技术服务工单》 | 按需提供 |
| 37 | 系统软件版本升级 | 在服务期内，针对维保范围的产品提供同代系统版本升级服务。由供应商对产品系统进行配置备份。在不影响业务系统正常运行的情况下，对产品系统版本进行升级，并完成新系统的配置恢复。新系统上线后，对网络连通性和业务可用性进行测试，保证业务的正常运行。  要求：需提供维保的安全产品原厂商授权书并加盖原厂商公章。 | 《系统版本升级记录》 | 按需提供 |
| 38 | 产品特征库升级服务 | 在日常运维的过程中，根据产品的性能对安全产品的特征库进行定期升级。在可升级的版本范围内，保证特征库及时更新。  要求：需提供维保的安全产品原厂商授权书并加盖原厂商公章。 | 《特征库升级记录》 | 按需提供 |
| 39 | 产品保修 | 在服务期内，若维保产品出现软硬件故障，需提供免费维修服务。保障设备及业务系统的持续可用性。 | 《产品故障分析报告》 | 按需提供 |
| 40 | 备机服务 | 具备完善、充足的备机配件库。维保范围的产品发生故障且短时间内无法修复时，需提供备机服务。在短时间内，将备机或备件送至现场进行更换。确保业务系统的正常运行。 | 《技术服务工单》 | 按需提供 |