## 网络安全风险评估和渗透测试服务需求

一、服务内容

|  |  |
| --- | --- |
| 1 | 风险评估服务：按照相关法规和标准的要求，结合采购人的具体情况，每季度对采购人指定的关键信息基础设施进行一次全面的安全风险评估，在网络系统受到危害之前为管理员提供专业、有效的安全分析和修补建议，并配合采购人的安全加固工作，对涉及版本升级或者安全手段建设方面的安全隐患，给出明确的加固建议和指导。服务频率：每季度1次，一共8次。 |
| 2 | 渗透测试服务:根据《中华人名共和国网络安全法》和《关键信息基础设施安全保护条例》中的要求，投标人在服务期内提供现场渗透测试，原则上立足于黑盒方式，模拟黑客的攻击思路与技术手段，从攻击者角度，发现应用系统存在的安全隐患，检测相关系统的威胁防御能力，深度挖掘应用系统的安全漏洞，为采购人指定的应用系统提供渗透测试服务，包括但不限于网站和重要业务系统等。服务频率：每半年1次，一共4次。 |
| 3 | 根据风险评估和渗透测试的结果分别进行修复或处置，处置后进行复测，复测后仍需形成复测报告。 |

二、具体工作要求：

**（一）风险评估工作要求**

 1、投标人须每季度对采购人指定的关键信息基础设施进行1次全面的安全风险评估。

 2、严格按照相关法规和标准的要求，结合采购人的具体情况，采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性，并综合安全事件严重程度，判断安全事件造成的损失对采购人的影响。投标人须提供风险评估所涉及的检测工具，为采购人指定的范围提供漏洞检测、安全基线核查等服务。服务期间，因检测工具产生的一切费用由投标人自行承担。

 3、投标人须为采购人提供网络层、系统层、应用层等层面的安全检测与评估，在提交风险评估报告后，投标人同时完成安全风险加固工作。在加固完成后对其进行复测，复测后提交复测报告。

 4、风险评估内容包括但不限于:

（1）安全设备状态检查

 查看安全设备的运行状态、设备负载等是否正常，同时对设备的版本进行检查，提出改进建议，经确认后，参与实施工作(根据实际情况升级等)。

（2）安全配置基线核查

 对主机、数据库、中间件、网络设备、安全设备等进行安全配置基线核查，检查内容包括但不限于系统版本补丁和基本信息、用户账号口令及身份、用户登录密码、系统授权验证、日志查看、系统网络应用配置等。通过对主机及应用系统日志记录、运行趋势进行分析，定期查验网络系统当前存在的安全防护薄弱环节，查找系统被入侵痕迹，查验系统可能存在的安全隐患。

（3）安全漏洞扫描

 对系统中的各种软硬件设备可能存在的安全漏洞问题进行扫描，扫描的对象包括系统中关键的服务器、网络设备、安全设备、商用软件及应用开发软件，扫描的范围包括但不限于以下内容:能够扫描发现网络设备、服务器(windows、linux、AIX)、防火墙、数据库、中间件、安全设备、应用开发软件中的安全漏洞。能够全面发现信息系统存在的各种脆弱性问题，包括信息探测类、后门程序类、域名服务类、Web安全类等安全漏洞、安全配置问题、应用系统安全漏洞。

（4）Web安全检查

 根据web多层面组成的特性，通过对Web的每一个层面进行评估和综合的关联分析，查找Web站点中可能存在的安全问题和安全隐患。检查内容包括但不限于Web服务是否安装了不必要的组件、运行身份是否正确设置、版本信息是否隐藏、目录遍历功能是否启用、是否启用IP访问限制、是否启用SSL传输加密、是否启用了日志记录、是否进行了严格的权限设置等。

 5、风险评估报告:根据检查内容形成整体风险评估报告，报告包含漏洞详述和修补方案。在提交风险评估报告后，投标人同时完成安全风险加固工作。在加固完成后对其进行复测，复测后提交复测报告。

**（二）渗透测试服务工作要求**

 1、投标方应保证招标方信息系统正常运行前提下，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞，帮助招标方理解应用系统当前的安全状况，发现在系统复杂结构中的最脆弱链路并针对安全隐患提出解决办法，切实保证信息系统安全。

2、渗透测试服务包括但不限于:

（1）采购人授权后，投标方应通过模拟黑客攻击行为通过本地或远程方式对目标对象进行非破坏性的入侵测试。

（2）渗透测试应至少包括但不限于以下范围的漏洞：

1.WEB应用系统渗透

2.主机操作系统渗透

3.数据库系统渗透

（3）渗透测试内容包括但不限于：

1.身份验证类

2.会话管理类

3.访问控制类

4.输入处理类

5.信息泄露类

6.第三方应用类

3、投标方渗透测试人员应针对使用不同技术手段发现不同维度的漏洞，并进行验证，形成记录和报告。

4、投标方渗透测试人员应在招标方授权许可的情况下以目标业务系统为跳板进行横向渗透，发掘更深层次的漏洞并展现漏洞被利用后的危害。

5、投标方应编写渗透测试报告并提交给招标方，报告应该阐明招标方业务系统中存在的安全隐患以及专业的漏洞风险处置建议，完成风险处置，提交最终处置报告。