网络安全运营服务

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **系统** | **服务内容** | | | **报价** |
| **一级服务内容** | **二级服务内容** | **三级服务内容** | 按总价报价，总价上限为42.84万元 |
| **道路运输监管系统** | 网络安全监控服务 | 巡检服务 | 安全漏洞扫描 |
| 风险评估服务 |
| 安全渗透测试服务 | / |
| 安全应急演练服务 | 应急保障及演练服务 | 应急预案开发与完善服务 |
| 安全应急演练服务 |
| 应急响应保障服务 |
| 网络安全攻防演练服务 | / |
| **省“两客一危一重”车辆智能监管系统** | 安全应急演练服务 | | |
| 安全漏洞扫描服务 | | |
| 日志安全审计服务 | | |
| 安全渗透测试服务 | | |
| 应急响应保障服务 | | |
| **其他** | 网络安全培训服务 | | |

1. 道路运输监管系统

（一）网络安全监控服务

通过巡检服务、渗透测试服务，满足交通厅的网络安全运营服务需求。

1.1 巡检服务

1.1.1 安全漏洞扫描

1.1.1.1 服务内容

利用专业的漏洞扫描工具定期通过对信息系统主机、应用系统、网络设备、安全设备等进行漏洞扫描和漏洞验证测试，结合各应用系统特点提出安全加固方案，全面提升信息系统的安全保障能力。

漏洞扫描和评估：对业务应用系统开展主机、中间件、数据库以及应用程序漏洞扫描，及时发现安全漏洞，作为安全加固工作输入；跟踪全球安全漏洞态势，在办公网络发起漏洞扫描工作，保证新型安全漏洞可以及时得到漏洞验证，及时发现新型漏洞对资产的影响情况；通过对新建设应用系统进行上线前漏洞扫描工作，提前发现系统安全漏洞，及时通知系统相关人员实施整改。

1.1.1.2 服务频率

每两月1次。

1.1.1.3 服务成果

《安全漏洞扫描报告》

1.1.2 风险评估服务

1.1.2.1 服务内容

采用文档收集，问卷调查，弱点分析，配置检查和评估管理工具结合等多种手段，开展一次风险评估服务。应完成安全需求调研、安全技术水平调研、安全威胁调研、安全威胁分析，总体风险分析、安全应对措施建议，并形成风险评估报告。评估内容如下：

1.业务要求和目标分析：分析业务对信息系统的要求和目标，如可用性要求、完整性要求和安全性要求等。针对不同的目标确定其优先级，得出重点保障的要求和目标。

2.威胁建模：针对重点保障的要求和目标，构建信息安全威胁模型。具体过程包括：分析可能的攻击者，对攻击者进行分类，并考虑各类攻击者可能利用的攻击方式、方法和途径。分析信息系统物理环境、网络平台、主机存储、系统部署结构可能面临的威胁等。依据构建的威胁模型，进行脆弱性分析。

3.风险分析针对重点保障的要求和目标，以及威胁模型分析情况，评估业务系统存在的风险，重点评估风险的不同级别。

4.风险控制措施对所有风险情况进行统计、分析及总结，提出有针对性的风险控制措施。针对综合运输服务子系统的总体情况，提出整体安全控制措施并形成完善解决方案，保障支撑业务安全目标的实现。

1.1.2.2 服务频率

服务期内1次。

1.1.2.3 服务成果

《风险评估报告》

1.1.3 服务人员要求

投入的服务人员含1名中级工程师（含中级及以上工程师）。

1.2 安全渗透测试服务

1.2.1 服务内容

渗透测试是指完全站在攻击者角度对目标系统进行的安全性测试过程。通过模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全性做深入的探测，发现系统最脆弱的环节，从而为综合运输服务子系统提供真实可信的安全风险描述。渗透测试一方面可以从攻击者的角度，检验业

务系统的安全防护措施是否有效，各项安全策略是否得到贯彻落实；另一方面可以将潜在的安全风险以真实事件的方式凸现出来，从而有助于提高相关人员对信息安全事件的认识水平。

渗透测试服务主要内容包括但不限于如下：

1.常规漏洞测试

（1）目录遍历：检测渗透测试目标针对用户输入的特殊字符是否具有限制功能，避免攻击者绕过限制能够访问任意文件的风险。

（2）SQL 注入：检测渗透测试目标针对用户输入的 SQL 命令是否具有过滤功能，避免攻击者将 SQL 命令注入到后端数据库引擎执行的风险。

（3）反射型 XSS：检测渗透测试目标针对用户输入的 Script 代码是否具有过滤措施，避免嵌入 Web 页面的 Script 代码被执行的风险。

（4）跨站伪造请求（CSRF）：检测渗透测试目标针对网络请求是否具有过滤功能，避免攻击者通过伪装请求来访问网站的风险。

（5）代码注入：检测渗透测试目标针对 PHP 代码是否具有过滤功能，避免攻击者构建特殊 PHP 代码注入到网站后端运行的风险。

（6）LDAP 注入：检测渗透测试目标针对输入的 LDAP 命令是否具有过滤功能，避免攻击者可能直接访问 LDAP 目录数据库的风险。

（7）XML 注入：检测渗透测试目标针对输入的 XML 代码是否具有过滤功能，避免攻击者输入恶意的代码来执行自身权限以外功能的风险。

（8）意外文件格式上传：检测渗透测试目标针对上传的文件是否具有过滤功能，避免攻击者构造特殊文件上传至服务器的风险。

（9）登出会话遗留：检测渗透测试目标针对会话 session 是否具有限制功能，避免服务器资源被大量消耗或会话重放等风险。

（10）任意文件下载：检测渗透测试目标针对文件下载是否具有限制功能，避免攻击者能够查看或下载任意文件。

2.中间件漏洞测试

（1）Tomcat 未授权访问：检测渗透测试目标针对 Tomcat 访问具有限制功能，避免攻击者未授权访问 Tomcat 的风险。

（2）Weblogic 漏洞：检测渗透测试目标是否存在 WebLogic 反序列化等安全漏洞，避免攻击者绕过限制执行远程命令攻击的风险。

（3）Struts2 漏洞：检测渗透测试目标是否存在 Struts2 漏洞情况，避免系统存在被远程任意代码执行的风险。

（4）JBoss 漏洞：检测渗透测试目标使用的 JBoss 是否存在漏洞，避免攻击者攻击 JBoss 服务的风险。

（5）WebSphere 漏洞：检测渗透测试目标使用的 WebSphere 是否存在漏洞，避免攻击者攻击 WebSphere 服务的风险。

（6）IIS 漏洞：检测渗透测试目标使用的 IIS 是否存在漏洞，避免攻击者攻击 IIS 服务的风险。

（7）php-fpm 未授权访问漏洞：检测渗透测试目标针对 PHP-FPM 访问是否具有限制功能，避免攻击者构造 fastcgi 协议执行任意代码的风险。

（8）Redis 未授权访问：检测渗透测试目标针对 Redis 访问是否具有限制功能，避免攻击者使用 root 账户写入 SSH 公钥文件，从而直接通过SSH 登录服务器的风险。

（9）Memcache 未授权访问：检测渗透测试目标针对 Memcache 访问是否具有限制功能，避免攻击者未授权访问 Memcache 的风险。

（10）MongoDB 未授权访问：检测渗透测试目标针对 MongoDB 访问是否具有限制功能，避免攻击者未授权访问 MongoDB 的风险。

（11）Phpmyadmin 测试：检测渗透测试目标 Phpmyadmin 安全配置情况，避免攻击者攻击 phpMyAdmin 服务的风险。

（12）中间件弱口令：检测渗透测试目标使用的中间件是否存在弱口令的情况，避免攻击者暴力破解口令从而获得系统权限的风险。

3.业务安全测试

（1）弱口令：检测渗透测试目标在处理帐号注册环节是否具有口令强度限制功能，避免用户可以使用弱口令注册，造成用户帐号被轻易暴力破

解的风险。

（2）平行/垂直越权：检测渗透测试目标在权限处理环节是否具有限制功能，避免攻击者横向或纵向越权操作带来的风险。

（3）密码重置漏洞：检测渗透测试目标在密码重设和密码找回环节是否存在缺陷，避免攻击者能够重置用户密码的风险。

（4）会话超时检测：检测渗透测试目标是否具有会话有效时间限制功能，避免攻击者能够利用会话进行攻击的风险。

（5）登陆错误限制：检测渗透测试目标针对密码登录错误的次数是否具有限制功能，避免攻击者进行暴力破解的风险。

（6）验证码测试：检测渗透测试目标是否有验证码机制以及验证码机制是否完善，避免攻击者进行暴力破解的风险。

（7）重放攻击：检测渗透测试目标在身份认证等过程是否具有过滤及限制功能，避免攻击者进行重放攻击（Replay Attacks）的风险。

4.通信安全测试

（1）HTTP 测试：检测渗透测试目标针对不必要的 HTTP 方法（如DELETE、PUT、TRACE、MOVE、COPY）具有限制功能，避免 HTTP受攻击面变大的风险。

（2）HTTPS 证书校验错误：检测渗透测试目标 SSL 证书的兼容性、证书配置、证书过期等情况，避免系统证书被攻击的风险。

（3）不安全的 SSL/TLS：检测渗透测试目标 SSL/TLS 配置情况，避免信息在客户端被拦截和篡改的风险。

（4）URL 携带敏感信息：检测渗透测试目标在通信过程中的 url 参数中是否带有明文敏感信息，避免信息泄露的风险。

5.服务器安全测试

（1）端口检测：检测渗透测试目标端口开放的情况，避免不必要的端口被恶意攻击的风险。

（2）FTP 弱口令匿名访问：检测渗透测试目标 FTP 是否存在弱口令或匿名登录漏洞，避免攻击者破解 FTP 口令或者匿名访问 FTP 服务的风

险。

（3）操作系统漏洞：检测渗透测试目标操作系统是否存在漏洞未修复的情况，避免攻击者利用漏洞可以实现远程代码执行控制操作系统、提升

权限等风险。

（4）数据库漏洞：检测渗透测试目标数据库是否存在漏洞未修复的情况，避免攻击者利用漏洞窃取数据库信息。

（5）远程登录漏洞：检测渗透测试目标是否开启了远程连接以及远程连接是否具有限制功能，避免攻击者能够远程登录的风险。

6.信息泄露测试

（1）管理后台泄露：检测渗透测试目标是否存在管理后台泄露的情况，避免管理后台成为攻击者暴力破解目标的风险。

（2）错误信息泄露：检测渗透测试目标针对用户输入的特殊数据是否具有过滤功能，避免系统报错信息泄露敏感信息的风险。

（3）配置文件泄露：检测渗透测试目标重要配置文件读写权限的设置情况，避免系统文件被攻击者读取造成敏感信息泄露的风险。

（4）源码泄露：检测渗透测试目标是否存在源代码泄露的情况，避免攻击者通过分析源代码寻找系统隐藏漏洞的风险。

1.2.2 服务频率

服务期内2次。

1.2.3 服务成果

《安全渗透测试报告》

1.2.4

投入的服务人员含2名中级人员（含中级及以上人员）。

（二）安全应急演练服务

提供安全应急演练服务，满足交通厅的网络安全运营服务需求，如在“粤盾”攻防演练等过程中提供支撑。

2.1 应急保障及演练服务

2.1.1 应急预案开发与完善服务

2.1.1.1 服务内容

根据国家标准、结合业务信息系统需要，持续进行总体应急预案编制和完善工作。同时针对各具体场景进行专项预案编制工作。信息系统的运转离不开 IT 设备的可靠运行，在业务影响分析服务中识别出了支撑业务运作所需的 IT 资源有哪些，因此需要针对关键业务所需的所有 IT设备，都将为之编制应急恢复预案，用于这些关键 IT 设备发生故障或失效时能够快速的恢复正常运行。应急预案编制范围与数量由三部分内容组成：

1.根据风险分析服务所识别出的重大风险，设计能有效应对的应急预案。这部分应急预案属于事件导向数量目前难以确定，以满足重大风险必须有应急预案为原则；

2.根据通用或标准事件类别，将结合信息系统实际需要，设计针对这些事件类别的应急预案；

3.所有在业务影响分析服务中识别出的支撑重要业务所需的关键IT 设备，都将为之编制应急恢复预案。这部分应急预案属于设备导向，以满足关键设备必须有应急恢复预案为原则。

应急预案的编制将从两个维度来展开：一个维度是从信息系统所面临风险从而可能发生的事件角度来编制相应的应急预案，这里的应急预案的也要考虑该事件所影响的信息系统范围，但由于事件发生的不确定性，更多的是侧重于事件处置流程的确定；另一个维度是从设备运行所面临的故障或性能降级角度来编制相应的应急恢复预案，这里的应急恢复预案较少考虑导致设备故障的原因，更多的考虑设备恢复的时间要求以及相应的应急资源情况。

2.1.1.2 服务频率

服务期内持续完善总体应急预案，针对具体场景编制 1 个专项应急预案。

2.1.1.3 服务成果

《应急总体预案》

《指定场景专项预案》

2.1.2 应急演练服务

2.1.2.1 服务内容

为保证应急响应措施有效落实，根据综合运输服务子系统网络架构和信息系统应用情况结合实际情况制定信息安全应急演练方案，然后根据应急演练方案在服务期内开展一次应急演练。通过不断的应急演练，不断完善应急响应流程及机制，检验重要信息系统应急管理有效性，提高各级人员的应急意识及应急处理实战能力，建立与上级主管部门应急协调机制。演练内容包括运行环境安全、网络结构安全、设备运行安全、系统可用性、外界风险因素等各方面，达到全面演练和专项演练相结合。演练形式以模拟实战演练为主，需制定演练方案和演练计划，按照演练方案和计划进行部署，具体要求如下：

1.制定详细的演练方案，明确演练目标、参加演练的信息系统、涉及的形式、层次和范围，设定灾难情况、演练流程、操作内容、应急资源、进度安排、演练的风险及其应对措施。

2.配备专职人员负责应急演练工作，组建应急团队，组建应急演练通讯、指挥体系，制定应急响应流程，制定应急恢复策略。

3.演练前做好各项准备工作，组建应急团队、指挥通讯体系，培训参演人员，确保组织、人员、资源到位。演练过程中要做好事前和事后对内、对外的联系和通知工作。

4.加强对演练工作的风险管理，审慎开展应急演练，严格控制应急演练引起的信息系统变更风险，避免因演练导致服务中断。演练前应对应急预案进行认真审核和修改完善，确保应急预案内容切实可行；应认真评估演练本身可能带来的风险和对业务的影响，制定完善的保障措施和应急回退方案。

5.应急演练完成后应对演练进行评估，编写急演练总结报，并根据演练评估结论对应急预案进行维护和更新。

2.1.2.2 服务频率

服务期内1次。

2.1.2.3 服务成果

《应急演练脚本》

《应急演练讲解 PPT》

《应急演练总结报告》

2.1.3 应急响应保障服务

2.1.3.1 服务内容

当信息系统、网络设备系统发生业务中断、网络瘫痪、大规模病毒爆发、主机异常、数据丢失等重新安全事故时，需要信息安全服务商提供应急响应服务，快速排查故障，分析事故源由，制定安全应对建议，恢复网络、信息系统、数据运行。应急响应服务方式为远程响应和现场服务，利用相关的应急响应安全策略生成工具，对突发安全事件提供 7\*24 小时的电话技术支持，在工作时间内半小时响应，2 小时内到达现场，非工作时间内 4 小时到达现场。在处理紧急事件时，通常先尝试通过远程接入的方式定位并解决问题，如果条件不允许或不能解决问题，将尽可能快的赶赴事件现场进行处理。协助快速解决问题，保证系统的正常稳定运行。现场应急服务服务期内不超过 2 次，远程应急技术支持服务为服务期内提供电话和远程操作技术支持服务。应急服务内容为：

1.协助系统运维单位开展系统故障检测

2.协助系统运维单位开展系统故障排除

3.协助系统运维单位开展隔离关键数据

4.协同系统运维单位攻击手段分析，提供应急方案或工具软件

5.协同系统运维单位定位攻击来源，提出安全建议

6.协助系统运维单位开展数据及网络业务恢复

7.协助系统运维单位开展系统调试、恢复

2.1.3.2 服务频率

服务期内不超过2次。

2.1.3.3 服务成果

《应急响应处置报告》

2.1.4 服务人员要求

投入的服务人员含1名中级人员（含中级及以上人员）。

2.2网络安全攻防演练服务

2.2.1服务内容

在省监管部门举行全省攻防演练活动时，在指定环境中进行安全防守的演练活动，根据道路运输监管系统实际情况调研并制订安全防守方案，从安全技术、管理和运营等多个维度着手，发现安全防御能力的问题和缺陷，防守方使用工具和安全设备进行观察，监控并掌握攻击方进行防守；主动提供安全加固服务，包括但不限于威胁监测与响应、Web防护、网络流量分析、漏洞管理、日志分析和蜜罐防护等；协助系统运维单位对攻击点进行紧急加固和处置，防疫各种风险漏洞，形成《防守成果报告》和《防守总结报告》，通过日常实战性攻防演练，进一步查找网络安全风险点，提升中心整个网络的安全性和可靠性。

2.2.2服务频率

服务期内按需要响应，服务次数不多于 2 次。

2.2.3 服务成果

《安全演练方案》

《安全演练总结报告》

2.2.4 服务人员要求

投入的服务人员含1名中级人员（含中级及以上人员）。

1. 省“两客一危一重”车辆智能监管系统

（一）安全应急演练服务

1.1 服务内容

应急演练将通过模拟网络攻防对抗的方式，验证用户当前各项防护措施能否对网络入侵做到准确的识别、发现以及响应。同时，通过真实的网络对抗的方式，能够模拟攻方可能采取的入侵路径，并检验应急响应的处置流程是否合理，参与各方是否熟练掌握应急处置流程步骤，针对性的修改应急预案。

安全攻防演练服务流程如下：

1.应急预案编制

2.模拟环境搭建

3.应急演练

4.总结汇报

为了确保演练安全、有效地进行，演练所遵循的基本原则如下：

1.充分考虑最有可能发生的紧急事件场景。

2.由于时间和空间的限制，选取具有代表性和概括性的场景进行演练。

3.在有限的时间内进行最基本的和最重要的场景演练。

4.保证整个演练过程的风险可控。

5.尽可能多的操演应急处置过程的各个环节。

6.演练的过程既要达到演练的目的，又要尽可能保证演练对信息系统正常运营的影响降到最低。

通过应急演练服务，能够有效检验系统应急预案以及系统应急演练方案的完善性和指导性，完善网络与信息安全专项应急预案及现场处置方案、改进应急操作及流程，全面提高组织的应急响应能力、流程运转能力。具体如下：

1.验证能力与流程

验证应急管理组织和人员的协调、协同操作及沟通能力；

验证应急管理组织对应急处置流程的执行和控制能力；

验证现场处置流程/方案的完整性、有效性和可操作性；

2.发现不足

通过演练过程，发现应急处置流程/预案等方面存在的问题和不足并加以改进；

3.锻练团队

使应急组织架构的人员熟悉、了解相关的策略、流程和方法；

使技术人员能进行实际切换操作，掌握相关的技术和规程；

使各个应急相关部门人员通过实际演练，明白在应急状况下，各自行使的职能,承担的职责和需要完成的任务；

使组织及下属单位提高应急响应的综合执行能力。

提供1次应急演练，演练场景不超过5个。

1.2 服务频率

服务期内1次。

1.3 服务成果

安全攻防演练服务主要工作产出物包括以下成果：

|  |  |  |
| --- | --- | --- |
| 服务内容 | 服务成果 | 数量（份） |
| 应急攻防演练 | 《应急总体预案》（如有更改/更换） | 1 |
| 《预案演练记录》 | 1 |
| 《应急演练总结报告》 | 1 |

1.4 服务人员要求

投入的服务人员含1名中级工程师（含中级及以上工程师）。

（二）安全漏洞扫描服务

2.1 服务内容

1.多种检查能力合一，全面系统脆弱性发现

漏洞扫描服务能够全方位检测信息系统存在的脆弱性，发现信息系统存在的安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。

2.风险统一分析

目前市场上有很多独立的漏洞扫描、配置检查、Web应用扫描产品，对信息系统进行安全检查后，分别得到不同的检查报告，互相之间没有联系，实际上不同脆弱性的扫描结果都从不同方面反映网络系统的安全风险状态，要了解信息系统总体安全风险状况，需要对脆弱性的所有方面统一进行分析和评估。

3.结合资产从海量数据快速定位风险

漏洞扫描服务能尽量收集信息系统环境信息，建立起信息系统资产关系列表。准备工作完成后，系统基于资产信息进行脆弱性扫描和分析报告。脆弱性扫描分析结果以仪表盘方式展示，从风险发生区域、类型、严重程度进行不同维度的分类分析报告，用户可以全局掌握安全风险，关注重点区域、重点资产，对严重问题优先修补。对于需要定位主机安全脆弱性的安全维护人员，通过直接点击仪表盘风险数据，可以逐级定位风险，直至定位到具体主机具体漏洞。远程安全评估系统也提供了强大的搜索功能，可以根据资产范围、风险程度等条件搜索定位风险。

4.识别非标准端口，准确扫描服务漏洞

漏洞扫描服务应用先进的非标准端口识别技术、以及丰富的协议指纹库，能够快速准确的识别非标准端口上的应用服务类型，并进一步进行漏洞检测，极大的避免了扫描过程中的漏报和误报。

2.2 服务频率

每季度1次。

2.3 服务成果

应用漏洞扫描服务主要工作产出物包括以下成果：

|  |  |  |
| --- | --- | --- |
| 服务内容 | 服务成果 | 数量（份） |
| 应用漏洞扫描 | 《系统漏洞扫描报告》 | 4 |

2.4 服务人员要求

投入的服务人员含2名中级工程师（含中级及以上工程师）。

（三）日志安全审计服务

3.1 服务内容

网络、安全设备是信息流通的必然结点，每个网络设备都会产生相应的日志信息，通过对日志信息的全面、深入分析，可以了解设备的工作状况，网络状况以及安全事件等信息。但是，目前网络设备越来越多，网络攻击的手段越来越多样，攻击方法越来越隐蔽，单纯的依靠某一种安全设备的事件来对网络安全情况进行评估和反应是远远不够的。根据等级保护基本要求，要对各类系统产生的安全日志实现全面、有效的综合分析，就必须为网络安全管理员建立一个能够集中收集、管理、分析各种安全日志的安全审计管理中心，把管理员从庞杂的日志信息分析中解放出来，为管理员提供一个方便、高效、直观的审计平台，大大提高了安全管理员的工作效率和质量，更加有效地保障了网络的安全运行。通过部署安全审计系统实现以下策略以保证网络的安全性。

1.日志集中管理策略：收集信息系统中各种网络设备、系统的日志信息，包括设备运行状况、网络流量、用户行为等信息，进行统一集中存储。

2.审计分析集中展示策略：提供多样、灵活的日志信息查询，包括事件的日期和时间、用户、事件类型、事件结果等条件进行查询，并把不同设备及平台的事件关联起来，帮助管理员实现更加全面、深入的分析事件。支持将事件进行详尽的分析及统计的基础上支持丰富的报表，实现分析结果的可视化。

3.多种网络设备的日志收集：支持安全设备（如防火墙，IDS、AV等）、网络设备（如router、switch）等多种产品及业务系统的日志数据的采集和分析。

4.自身安全策略：用户分级管理，严格限制各级用户的管理权限，同时对超级用户数量进行限制，密码采用强密码机制，避免管理用户的职权滥用。设置数据库的备份策略，定期备份导出数据，并且进行数据库上限及报警上限，避免数据库信息的不预期删除、覆盖和修改。

3.2服务频率

服务期内1次。

3.3服务成果

日志安全审计服务主要工作产出物包括以下成果：

|  |  |  |
| --- | --- | --- |
| 服务内容 | 服务成果 | 数量（份） |
| 日志安全审计服务 | 《日志安全审计分析报告》 | 1 |

3.4服务人员要求

投入的服务人员含1名中级工程师（含中级及以上工程师）。

（四）安全渗透测试服务

4.1 服务内容

以黑客的视角对应用系统的安全状况进行黑盒测试，使用黑客攻击的工具和手段对应用系统进行模拟攻击测试，挖掘可能存在的安全隐患。

1.信息收集：

收集目标系统的基本信息，包括IP地址、域名、子域名等。

分析目标系统所处的网络环境和拓扑结构，了解系统的架构和相关组件。

收集目标系统的相关文档、配置文件等，以获取更多有关系统的信息。

2.渗透测试

检测范围至少包括：

（1）系统层安全测试：

* 远程溢出

远程溢出测试基于漏洞扫描的结果，一旦远程溢出被利用，攻击者很有可能就会获得系统的最高权限。

* 口令猜测

使用常见的密码对服务器系统进行远程密码猜解。包括系统密码，WEB等系统应用。

* 跳板攻击测试

攻击者控制同网段的一台主机后向目标主机进行入侵。

（2）应用层安全测试

* 系统结构分析及测试信息收集

信息收集工作包括WEB服务器和应用程序指纹探测、后台应用程序发掘、爬网和Googling、错误代码挖掘、应用程序配置管理测试等。

* 业务逻辑缺陷&程序逻辑缺陷

分析业务流程是否存在业务逻辑缺陷，程序中是否存在逻辑缺点，攻击者可通过缺陷实施攻击，越权访问操作他人数据、账号信息等。

* 登陆验证测试

验证是服务器与用户端建立身份和权限鉴别的过程。验证过程需要多个验证因素共同完成。验证测试工作包括缺省的或可猜测的（字典攻击）用户账户测试、验证旁路迂回测试、注销管理和浏览器缓存管理测试、弱密码测试等。

* 会话管理测试

会话管理测试主要集中于分析出会话管理机制，并针对每个步骤的安全性、令牌的脆弱性进行测试，来检测Web应用程序会话机制是否存在安全隐患，能否被非法利用（会话劫持，伪装成合法用户）而影响Web应用程序的安全。会话管理测试工作包括Cookie与Session令牌操纵测试、暴露的会话参数测试、跨站请求伪造测试。

（3）数据传输安全测试

对于涉及敏感信息或资金交易的数据传输，检测是否有加密，加密措施或协议，导致攻击者可以利用缺陷获取敏感信息或修改传输内容。同时检测数据传输是否有完整性校验。

（4）敏感信息保护

应用系统对于敏感数据：如密码、密钥、重要用户信息在内存中、缓存、临时文件等存放地方是否有加密保护，是否可能被破解、被窃取明文信息、非授权访问等。

（5）敏感信息泄露

通过工具或手工挖掘应用系统中存在敏感信息，包括目录遍历、隐藏文件、备份文件、任意文件下载等敏感信息泄露。

3、报告输出：

根据安全渗透测试结果进行分析，形成《安全渗透测试报告》。包括发现的漏洞、攻击路径、修复建议等信息。

4.2 服务频率

服务期内2次。

4.3 服务成果

安全渗透测试服务主要工作产出物包括以下成果：

|  |  |  |
| --- | --- | --- |
| 服务内容 | 服务成果 | 数量（份） |
| 安全渗透测试服务 | 《安全渗透测试计划》 | 1 |
| 《安全渗透测试报告》 | 1 |

4.4 服务人员要求

投入的服务人员含2名中级工程师（含中级及以上工程师）。

（五）应急响应保障服务

5.1 服务内容

当信息系统、网络设备系统发生业务中断、网络瘫痪、大规模病毒爆发、主机异常、数据丢失等重新安全事故时，需要信息安全服务商提供应急响应服务，快速排查故障，分析事故源由，制定安全应对建议，恢复网络、信息系统、数据运行。应急响应服务方式为远程响应和现场服务，利用相关的应急响应安全策略生成工具，对突发安全事件提供 7\*24 小时的电话技术支持，在工作时间内半小时响应，2 小时内到达现场，非工作时间内 4 小时到达现场。在处理紧急事件时，通常先尝试通过远程接入的方式定位并解决问题，如果条件不允许或不能解决问题，将尽可能快的赶赴事件现场进行处理。协助快速解决问题，保证系统的正常稳定运行。现场应急服务服务期内不超过 2 次，远程应急技术支持服务为服务期内提供电话和远程操作技术支持服务。应急服务内容为：

1.协助系统运维单位开展系统故障检测

2.协助系统运维单位开展系统故障排除

3.协助系统运维单位开展隔离关键数据

4.协同系统运维单位攻击手段分析，提供应急方案或工具软件

5.协同系统运维单位定位攻击来源，提出安全建议

6.协助系统运维单位开展数据及网络业务恢复

7.协助系统运维单位开展系统调试、恢复5.2 服务频率

服务期内不超过2次。

5.3 服务成果

《应急响应处置报告》

5.4 服务人员要求

投入的服务人员含1名中级人员（含中级及以上人员）。

1. 其他

（一）网络安全培训服务

1.1 服务内容

在服务期内，对中心负责信息化、系统运维单位、系统开发单位等相关人员进行网络安全知识培训，内容主要包括网络安全的基本知识，网络安全相关法律的解读，常见安全问题的应急处理方法等，实际可根据用户需求做相应调整。

通过培训，使有关人员能够对网络技术、信息安全等相关知识有系统的、全面的了解和认识，进一步提高人员的安全意识，强化人员的网络安全观念。

1.2 服务频率

服务期内1次。

1.3 服务成果

交付成果包含不限于相关的网络安全知识培训课件、培训材料和签到表等。

1.4 服务人员要求

投入的服务人员含1名中级工程师（含中级及以上工程师）。