达州市公安局安全服务项目

服务需求说明书

目 录

[第一章 常规安全检测服务需求 3](#_Toc104717241)

[1.1 风险评估 3](#_Toc104717242)

[1.1.1 服务内容 3](#_Toc104717243)

[1.1.2 服务方式 8](#_Toc104717244)

[1.1.3 交付成果 13](#_Toc104717245)

[第二章 安全运维服务需求 14](#_Toc104717246)

[**2.1** **安全监测服务** 14](#_Toc104717249)

[2.1.1 服务概述 14](#_Toc104717250)

[2.1.2 服务内容 14](#_Toc104717251)

[2.1.3 服务方式 15](#_Toc104717252)

[2.1.4 交付成果 15](#_Toc104717253)

[**2.2** **应急响应服务** 15](#_Toc104717254)

[2.2.1 服务概述 15](#_Toc104717255)

[2.2.2 服务内容 16](#_Toc104717256)

[2.2.3 服务方法 17](#_Toc104717257)

[2.2.4 交付成果 17](#_Toc104717258)

[**2.3** **应急演练服务** 18](#_Toc104717259)

[**2.4** **安全培训服务** 18](#_Toc104717260)

[**2.5** **病毒防护服务** 19](#_Toc104717261)

[附件：服务工作清单 20](#_Toc104717262)

# 常规安全检测服务需求

* 1. **风险评估**

风险评估对象为达州市公安局现有信息系统。

### 服务内容

#### 技术评估

1. **资产评估**

保护达州市公安局信息系统资产免受安全威胁是本次安全服务的根本目标。要做好这项工作，首先需要详细了解资产分类与管理的详细情况。

表1资产分类调查表

|  |  |
| --- | --- |
| **项目名称** | **资产分类调查** |
| 简要描述 | 采集资产信息，进行资产分类，划分资产重要级别； |
| 达成目标 | 采集资产信息，进行资产分类，划分资产重要级别；  进一步明确评估的范围和重点； |
| 主要内容 | * 采集资产信息，获取资产清单； * 进行资产分类划分； * 确定资产的重要级别； |

表2资产分级调查表

|  |  |
| --- | --- |
| **项目名称** | **资产管理** |
| 简要描述 | 评估资产的安全等级和应给予的安全保护等级 |
| 达成目标 | 评估资产的安全等级；  评估资产应给予的安全保护等级； |
| 主要内容 | * 确定资产的安全等级； * 对安全保障进行等级分类； * 确定资产的应给予的保护级别； |

1. **网络结构评估**

对达州市公安局网络结构进行全面的分析，发现现行网络结构存在的风险和安全问题以及对提供相应的调整建议。

|  |  |
| --- | --- |
| **项目名称** | **网络结构分析** |
| 简要描述 | 网络结构的风险评估是针对用户的网络结构进行分析，根据达州市公安局的安全需求查找相应的安全脆弱性，最终提交详尽的报告和相应的建议。 |
| 达成目标 | 通过网络结构的风险评估，可以知悉当前网络结构的安全脆弱性 |
| 主要内容 | * 调查安全需求 * 分析网络结构 * 当前网络结构的安全脆弱性 * 可能存在的安全风险 * 网络结构中需要改进的方面 * 网络安全域评估分析 |

1. **主机评估**

对达州市公安局服务器、终端、数据库、网络设备及安全设备进行全面的分析和评估，发现系统中存在的风险和安全问题并提供相应的调整建议。

表3主机安全评估表

|  |  |
| --- | --- |
| **项目名称** | **主机安全评估** |
| 简要描述 | 主机安全评估是针对用户的服务器、终端、数据库、网络设备及安全设备进行全面分析评估，最终提交详尽的报告和相应的建议。 |
| 达成目标 | 通过主机安全评估，可以知悉当前系统安全脆弱性。 |
| 主要内容 | * 补丁管理 * 最小服务原则 * 最大安全性原则 * 帐户安全管理 * 口令安全管理 * 日志安全管理 * 入侵管理 |
| 实现方式 | * 工具扫描 * 人工评估 * 人员访谈 |

1. **应用系统评估**

* 服务描述

对应用系统进行安全评估，从应用系统的开发、安装部署、网络通讯、认证授权、安全审计、备份容错、运行维护等进行评估，鉴别应用系统所存的风险，并且提供详尽的报告和详尽的建议。

通过对应用系统的风险评估，使达州市公安局可以：

* 知悉已有应用系统平台自身和运行维护中存在的弱点，为安全整改提供意见
* 对新接入应用系统进行安全检察，对符合安全要求的方进行准入，保证新接入系统的安全性
* 为正在规划的应用系统提供安全方面的意见，从应用系统规划时即进行安全考虑
* 服务内容

对应用系统的安全服务涵盖了（但不仅限于）以下的内容：

表4应用系统评估内容表

|  |  |
| --- | --- |
| **类别** | **内容描述** |
| 应用开发 | * 检查自开发的应用系统采用了合理的编程方式、习惯 * 检查应用系统的开发、测试和生产运行环境是否分离 |
| 安装部署 | * 查看应用系统采用的系统架构、软硬件支持环境、层次模型等信息 * 检查支撑平台（操作系统、数据库等）的安全保护措施是否适当 * 应用系统的开发、测试和生产运行环境是否分离 * 应用系统与其它应用系统共用同一主机、数据库等支撑环境 |
| 网络通信 | * 检查用户与服务器、服务器与服务器之间的信息传输是否有安全性保密措施 |
| 认证授权 | * 检查应用系统是否采用了合理的用户权限划分机制，帐户口令管理策略，用户的访问控制措施如何 * 当采用多因素验证时，服务器端的用户验证信息存储是否符合保密性、安全性、完整性 |
| 安全审计 | * 应用系统是否有审计（日志）系统 * 审计记录的用户对象是否包括所有的普通用户和管理员 * 审计记录的内容是否完善 * 审计的内容是否容易查看 * 审计查阅的周期是否合理 * 审计的存储是否有一定的保护措施，保障其保密性、完整性、可用性 |
| 备份容错 | * 应用系统是否采用了适当的备份、恢复和系统容错机制来保障系统的可用性 |
| 运行维护 | * 应用系统的安装、运行文档是否准确健全 * 是否建立可行的日常工作流程和应急恢复流程 * 是否能够安装相应的管理制度执行 |

#### 管理评估

安全管理和安全策略密不可分，安全管理是依据安全策略进行实施，对安全管理的评估往往从安全策略开始，主要包括：

* 达州市公安局网络系统安全策略；
* 技术标准和规范；
* 组织机构和人员职责；
* 安全操作流程；
* 管理规定和办法；
* 用户协议；
* 培训资料和用户手册；

安全管理评估首先从整体上对安全管理策略进行评估，然后再从常规安全管理与应急安全管理两个方面进行评估。

表5安全管理策略评估表

|  |  |
| --- | --- |
| **项目名称** | **安全管理策略评估** |
| 简要描述 | 评估现有安全管理策略的完善程度、合理程度； |
| 达成目标 | 依据风险管理的相关国内国际标准；  结合网络的实际业务与应用状况；  符合达州市公安局的实际需求，协助达州市公安局改进安全管理措施 |
| 主要内容 | * 人员组织安全管理 * 安全规章制度 * 安全策略方针 |
| 实现方式 | * 调查分析   + 问询式调查   + 《人员和安全管理调查表》 * 广泛交流   + 查阅相关管理制度；   + 与相关管理人员进行交流； |

表6常规安全管理评估表

|  |  |
| --- | --- |
| **项目名称** | **常规安全管理** |
| 简要描述 | 评估达州市公安局网络常规安全管理现状，分析其完善程度和合理程度； |
| 达成目标 | 依据风险管理的相关国内国际标准；  贴近达州市公安局网络的实际业务与应用状况；  结合达州市公安局的实际需求，协助达州市公安局改进常规安全管理措施。 |
| 主要内容 | * 业务应用安全管理 * 物理安全管理 * 设备安全管理 * 数据安全管理 * 开发维护管理 |
| 实现方式 | * 调查分析   + 问询式调查   + 《物理环境调查表》   + 《安全技术保障措施调查表》   + 《业务状况调查表》 * 广泛交流   + 与相关业务管理人员进行交流； |

表7应急安全管理评估表

|  |  |
| --- | --- |
| **项目名称** | **应急安全管理** |
| 简要描述 | 评估达州市公安局网络的应急安全管理现状，包括应急流程、步骤、能力和管理制度等 |
| 达成目标 | 准确评估达州市公安局网络的应急安全管理状况；  协助达州市公安局提高应急安全能力； |
| 主要内容 | * 应急案例 * 应急安全流程 * 应急安全步骤 * 应急安全能力 * 应急管理制度 |
| 实现方式 | 调查交流 |

### 服务方式

#### 漏洞扫描

漏洞扫描主要是根据已有的安全漏洞知识库，模拟黑客的攻击方法，检测网络协议、网络服务、网络设备、应用系统等各种信息资产所存在的安全隐患和漏洞。扫描的方式可以采用工具进行网络扫描。

利用安全扫描工具扫描网络中的核心服务器及重要的网络设备，包括服务器、交换机、防火墙等，以对网络设备进行安全漏洞检测和分析，对识别出的能被入侵者利用来非法进入网络或者非法获取信息资产的漏洞或脆弱性执行记录，并提醒安全管理员，及时完善安全策略，降低安全风险。

**扫描策略**

提供可定制的扫描策略的策略编辑器。按照扫描强度，默认的扫描策略模板包括：

* 高强度扫描
* 中强度扫描
* 低强度扫描
* 按照扫描的漏洞类别，默认的扫描策略模板包括：
* NetBIOS漏洞扫描
* Web&CGI漏洞扫描
* 主机信息扫描
* 帐户扫描
* 端口扫描
* 数据库扫描

在远程扫描过程中，将对远程扫描的目标按照操作系统类型和业务应用情况进行分类，采用定制的安全的扫描策略。

**数据分析及报告**

扫描结果存为统一格式进行统一分析和归类，并通过安全信息库系统进行数据分析，最终生成报告。

* 阶段报告，在扫描会话完成之后，由工具输出扫描报告，对原始数据进行整理生成原始数据报告
* 最终报告，通过人工分析最后形成远程扫描报告。

在进行远程扫描之后，扫描工具可输出原始数据报告，经数据库统计归类和人工分析之后，形成最终扫描报告。

#### 配置核查

安全漏洞通常是系统自身的问题引起的安全风险，反映了系统自身的安全脆弱性，安全配置通常都是由于人为的疏忽造成，主要包括了账号、口令、授权、日志、IP通信等方面内容，同样反映了系统自身的安全问题，但成因是不同的。安全配置与系统的安全性关联非常大，同一个配置项在不同业务环境中的安全配置要求是不一样的，因此在设计业务系统安全基线的时候，安全配置是一个关注的重点。通过配置核查减少攻击面、提高漏洞容忍度、提升防御强度。

配置核查的根本目的是依据设备的部署环境、承载业务等因素，逐条核查是否满足基本安全配置要求的合集，并给出指导加固方案，可作为设备入网、业务上线、日常运维、定期巡检的权威指南。

#### 人工评估

人工评估服务利用专业安全技术和相关知识，通过对主机或设备的操作与检查，收集了解主机或设备目前版本和补丁信息、系统配置、日志纪录等内容，针对这些信息进行技术分析，确定主机或设备目前的安全现状。

人工评估服务的目的包括以下内容：

* 对现有主机设备的安全现状（包括补丁，权限，安全特性等）进行了解，包括：是否存在的安全漏洞，这些安全漏洞是否严重，系统配置是否满足安全要求等；
* 检查系统是否有被攻击或入侵，主要包括对操作系统或应用系统、数据库的审计，确认系统是否被非授权用户获得权限或系统被非正常使用；
* 对安全系统进行专业的检查，看是否得到了正确的使用，以及相关的事件是否对系统有影响，审计的对象包括：防火墙，防病毒，入侵检测等安全设备；
* 主机系统评估

对于主要的操作系统或者应用来说，将主要从下面几个方面来获取系统的运行信息：

* 账号；
* 资源；
* 系统；
* 网络；
* 审核、日志和监控；

比如对于主机操作系统，这些信息主要包括：网络状况、网络配置情况、用户账号、服务配置情况、安全策略配置情况、文件系统情况、日志配置和纪录情况等。当然，对于特殊应用或者系统来说，将同应用联系更加密切，比如，数据库的身份验证方式，数据库文件保存的安全性等。

在技术审计过程中，维护单位应采用多种技术来进行信息收集，这些技术包括：

* 审计评估工具。通过相应审计评估脚本工具，通过执行该工具，就可以获取系统的运行信息。
* 常见后门分析工具。通过使用专业工具，检查系统是否存在木马后门
* 深层挖掘技术。通过安全专家的深层挖掘，检查系统是否被安装了Rootkit等很难被发现的后门程序

收集了系统信息之后，维护单位将对这些信息进行技术分析，审计的结果按照评估对象和目标对结果从补丁管理、最小服务原则、最大安全性原则、用户管理、口令管理、日志安全管理以及入侵管理七个方面进行归类处理并评分。

表8主机评估检查表

| **评估目标** | **评估内容** |
| --- | --- |
| 补丁管理 | 检查系统、应用的版本情况、补丁安装情况 |
| 最小服务原则 | 检查系统、应用的服务运行配置情况，察看是否遵循最小服务原则 |
| 最大安全性原则 | 检查系统是否进行了安全配置或者是否采用了恰当的安全防护机制。 |
| 帐户安全管理 | 检查系统或应用中账号的配置情况，是否存在默认账号或者不必要账号 |
| 口令安全管理 | 检查系统的账号口令配置情况，是否有账号是弱口令。 |
| 日志安全管理 | 检查系统或应用的日志配置情况，是否有严格的日志配置或者日志服务器。 |
| 入侵管理 | 检查系统的安全漏洞情况，以及是否被入侵等。 |

这7个方面将能够充分体现系统目前的运行和安全现状。通过数字分数的形式，并结合资产的重要性，将能够很直观地表现出系统的情况。并且可以根据其中存在的缺陷，制定相应的解决办法。

* 网络安全设备评估

如今对网络安全设备的评估已渐渐成为安全评估的一个重要的环节。对网络安全设备的评估，并不是简单地指对网络安全设备日志的审计，而是对网络安全设备的功能、设置、管理、环境、弱点、漏洞等进行全面的评估。

* 评估条件

审计前需要明确以下内容：

* 网络安全设备的周围网络环境，保护对象，安全要求；
* 网络安全设备周围区域网络的流程图（包括内部和外部）；
* 路由配置；
* 网络安全设备及周围设备在网络上的名字和IP地址；
* 网络安全设备网络连接情况（网络安全设备每个网络界面的IP和邻近设备）；
* 有网络安全设备的最基本信息，比如生产厂家，版本，质量保障合同，管理员的姓名，24小时技术支持的电话号码，等等；
* 评估内容

查看网络安全设备的配置、环境、和运行情况。这其中包括逻辑的和物理的状况。要调查的至少应包括以下几个方面：

* 网络安全设备的操作系统及版本；
* 察看网络安全设备的内存（RAM）使用情况。看看是否经常处于满负荷状态。如果是，在审计报告中建议考虑增加内存；
* 察看网络安全设备的中央处理器使用情况。看看是否经常处于满负荷状态。如果是，在审计报告中建议更换机器或分流流量；
* 网络安全设备的管理是远程操作的。是不是任何IP都可以允许进行远程管理。如果是，一定要在审计报告中要求对IP加严格的限制；
* 检查网络安全设备的规则检查；
* 审计网络安全设备的日志；
* 对网络安全设备实施攻击测验，以测验网络安全设备的真实安全性。这需要最谨慎从事；
* 管理服务
* 提供策略变更建议
* 提供日志管理建议
* 提供审计服务

#### 人员访谈

评估人员通过与网络管理员、系统管理员、应用管理员和安全管理员现场沟通，了解用户在网络层、系统层、应用层和安全管理的安全现状，进而全方位的发现信息系统及网络存在的安全漏洞，为漏洞修补提供依据。

#### 专家分析

评估人员通过收集、审阅用户提供的各类资料，如现有的安全管理制度、流程，应用系统的网络拓扑、开发、部署、运行和维护文档，与应用系统相关的各关键设备的安装配置和维护等文档，进行综合全面的分析评估。

### 交付成果

**交付成果包括但不限于：**

《信息系统综合风险评估报告》

# 安全运维服务需求

2. 1. **安全监测服务**

### 服务概述

安全监测是指通过监测工具，对达州市公安局信息系统进行持续监测，并根据资产性能、资产可用性、安全事件、业务连续性等为达州市公安局出具周期性的安全监测报告，让用户掌握网络中的风险状况及安全趋势。

### 服务内容

“安全监测服务”主要包括以下几方面的内容：

* **安全监测**

通过监测工具软件，对全网设备数、设备可用率、性能情况进行监控，包括内存、CPU的异常波动，磁盘的异常使用，磁盘的异常暴增，各种设备CPU、内存的负载情况，重启次数等指标。

* **安全事件管理**

通过监测工具软件，收集全网安全设备的日志，并通过过滤、归并等方式，剔除掉无用的日志信息，同时通过关联分析，符合关联规则条件的日志产生告警。

* **业务管理**

通过监测工具构建业务拓扑并对业务拓扑中的每个资产设定关键性能指标及其每个指标的权重，针对关键性能指标，自动计算业务的整体性能指数。系统同时会自动计算业务的脆弱性指数和业务的威胁指数，连同业务性能指数，综合计算业务的健康度，并绘制出健康度随时间变化的业务健康曲线。

* **网络故障诊断**

监测工具具备基于故障树的网络故障诊断功能，根据网络故障沿网络拓扑水平传播的特性，通过对大量网络告警事件在拓扑空间中的分布，以及传播时间上的顺序，自动判别故障源，减少故障恢复事件。

### 服务方式

安全监测服务以年度服务为基准。在服务期内，以电子邮件的方式，每周发送“安全监测报告”到达州市公安局指定的电子邮箱。

### 交付成果

**交付成果包括但不限于：**

《安全监测报告》。

* 1. **应急响应服务**

### 服务概述

当达州市公安局的主机或网络正遭到攻击或发现入侵成功的痕迹，而又无法当时解决和追查来源时。维护单位应根据达州市公安局的要求，以最快的速度赶到现场，协助达州市公安局解决问题，查找后门，保存证据和追查来源。此项应急响应服务由维护单位响应安全技术服务小组负责。可以与达州市公安局自己的网络安全中心以及反应体系配合协作，共同完成对达州市公安局网络安全事件的应急响应和处理。

**安全事件分类和等级根据事件等级**

**安全事故**

1. 由于安全原因造成的网络通信物理或逻辑中断的事故。
2. 由于安全原因系统重要业务运行停止造成的事故。
3. 系统重要业务数据损坏。
4. 系统遭受入侵，机密数据外泄。
5. 因安全隐患可能会造成事故的现象。

**严重安全事件：**

1. 由于安全原因造成的网络通信物理或逻辑中断的严重故障。
2. 由于安全原因系统重要业务运行停止造成严重故障。
3. 系统部分重要业务数据损坏。
4. 系统遭受入侵，部分机密资料外泄。
5. 因安全隐患可能会造成故障的现象。

**一般安全事件**

由于安全隐患或系统遭受入侵、尝试性入侵但未造成不良后果的网络通信或系统业务运行中出现的一般故障，或利用本网发起的对其它网络的攻击。

安全事件包括但不限于以下内容:

1. 非授权访问:通过入侵的方式进入到未被授权访问的网络中；
2. 信息泄密:数据在传输中因数据被截取、篡改、分析等而造成信息的泄漏；
3. 拒绝服务:正常用户不能正常访问服务器提供的相关服务；
4. 系统资源被非法占用:如有非法进程运行,并占用大量的CPU处理时间；
5. 在系统日志中发现非法登录者；
6. 发现系统感染计算机病毒；
7. 发现有人在不断强行尝试登录系统；
8. 系统中出现不明的新用户账号；
9. 管理员收到来自其它站点系统管理员的警告信，指出系统可能被威胁；
10. 文件的访问权限被修改；
11. 因安全漏洞导致的系统问题；
12. DNS条目错误；
13. IP地址冒用；
14. 非授权人持有帐户密码或进入系统；
15. 其它的入侵和违反本实施细则的行为。

### 服务内容

应急响应根据对事件进行处理的地点分为：远程应急响应和现场应急响应。

我们针对以下情况提供应急响应服务并给出相应的结果。

* 操作系统漏洞修复
* 端口服务漏洞修复与组件加固
* 数据库安全
* 防火墙与交换机策略加固
* 数据恢复与入侵追踪
* 操作系统的整体性能优化
* 其它安全响应
* 反数据嗅探与会话劫持
* 数据库的隔离、备份
* 日志隔离备份
* 事故处理报告

响应服务完成后，维护单位向达州市公安局提供详细的处理报告，内容包括：事故原因分析、已造成的影响、处理办法、处理结果、预防以及改进建议等。

### 服务方法

在达州市公安局网络发生突发安全事件后，启动应急响应服务，维护单位提供紧急响应服务，包括远程应急响应和现场应急响应，维护单位应尽快的赶到现场，恢复网络的正常工作，并协助检查入侵来源，提供事故分析报告和安全建议及服务，为用户提供及时、全面的安全问题解决方案。

远程支持安全服务方式可以分为以下几种：

* 7\*24小时电话支持服务；
* E－MAIL支持服务；
* 当远程支持无法解决问题时，将派遣专业的紧急响应服务人员在第一时间到达达州市公安局所在地提供现场支持服务。
* 在服务期内，故障响应时间不超过5小时，故障解决时间不超过4小时，疑难问题在8小时内给出解决方案。

### 交付成果

**交付成果包括但不限于：**

《安全事件应急响应报告》

* 1. **安全加固服务**

定期找出的核心系统巡检、渗透或扫描结果对信息系统进行安全加固，加固方式包括但不限于对网络、Web应用、数据库、管理策略进行安全配置加固和安全设备进行配置优化，提高信息系统的安全防御能力。

### 服务内容

#### 安全加固对象

1. 各类型系统平台：Linux、Windows 2000/2003/XP/Vista、BSD、Solaris2.5-8等；
2. 网络设备：WAN/LAN；
3. 安全设备：防火墙、入侵检测、日志审计系统、堡垒主机、数据库审计系统等；
4. 数据库：SQL-Server、Oracle、Sybase等；
5. 管理策略。

#### 安全加固内容

包括但不局限于以下服务：

1. 操作系统加固服务
2. 数据库加固服务
3. 网站加固服务
4. 网络加固服务
5. 管理策略加固服务

### 服务方式

定期针对全网的主机和应用系统修补、加固、修补及优化、提供详尽的操作报告，即《安全加固报告》。

* 1. **应急演练服务**

维护单位应根据达州市公安局的要求，协助制定或完善应急预案，开展应急演练等活动。

修订和完善应急预案将包括现状调研、综合预案完善、专题预案完善、特定系统预案完善等工作内容。

根据应急预案规定的流程，协助达州市公安局进行相应的模拟演练，一方面使相关方熟悉应急响应流程，提高对安全事件的响应能力；另一方面验证预案正确性和适用性，进行总结分析，根据需要对应急预案进行修订。使得达州市公安局信息系统相关人员了解应急流程和自己的责任，在安全事件发生时，能够有条不紊地开展应急工作，最大程度降低安全事件带来的负面影响和损失。

根据安全事件应急预案，在达州市公安局信息系统发生安全事件时及时响应，执行应急响应流程，通过专家级的技术支持和快速响应，及时消除达州市公安局信息系统安全事故，减少损失和负面影响，提高达州市公安局信息系统业务连续性。

* 1. **安全培训服务**

根据达州市公安局的实际需求，维护单位应提供针对全员的信息安全意识培训，针对管理人员提供安全治理培训，针对技术人员提供安全攻防技术、安全开发、安全产品技术原理及安装部署等方面的培训。包括：

* 信息安全基础知识
* 边界安全、传输安全、内网安全的知识培训
* 针对评估结果和安全加固建议的培训讲解
* 日常安全运维规范培训
* 一般故障解决方法培训
* 故障分析培训
* 安全突发事件应急处理培训
  1. **病毒防护服务**

维护单位应根据达州市公安局的要求，建立一个多层次、全方位的防病毒体系，可以自动对网络内出现的病毒自动处理，保证达州市公安局内部的物理机、虚拟机、云平台的安全。

# 附件：服务工作清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **参数** | **单位** | **数量** |
| 1 | 风险评估 | 风险评估将对信息资产所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能性的评估。作为风险管理的基础，风险评估是组织确定信息安全需求的一个重要途径。将根据国家相应评估规范进行安全风险，得出最科学、可量化的风险等级评价，从而进行风险管理及资源优化。 | 年 | 3 |
| 2 | 安全监测 | 通过监测工具，对达州市公安局信息系统进行持续监测，并根据资产性能、资产可用性、安全事件、业务连续性等为达州市公安局出具周期性的安全监测报告，让用户掌握网络中的风险状况及安全趋势。 | 年 | 3 |
| 3 | 安全加固 | 1. 每年对以下系统、设备进行安全加固：1) 各类型系统平台：Linux、Windows 2000/2003/XP/Vista、BSD、Solaris2.5-8等； 2. 网络设备：WAN/LAN； 3. 安全设备：防火墙、入侵检测、日志审计系统、堡垒主机、数据库审计系统等（网御星云防火墙设备2台、网御星云入侵检测系统系统1套、网御星云入侵防护系统1套） 4. 数据库：SQL-Server、Oracle、Sybase等； 5. 管理策略； 6. 安全设备售后服务能力承诺加盖投标人及生产厂商鲜章。 | 年 | 3 |
| 2 | 应急响应 | 1. 7×24小时的应急响应服务1) 恶意程序事件，如：计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件等有害程序事件。 2. 网络攻击事件，如：后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件等网络攻击事件。 3. 信息破坏事件如：信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件等信息破坏事件。 4. 信息内容安全事件，如：违反宪法和法律、行政法规的信息内容安全事件；对与我单位相关事项进行讨论、评论、歪曲、造谣形成敏感的舆论热点，出现一定规模炒作的信息安全事件；违法组织串连、煽动集会游行的信息安全事件等信息内容安全事件。 5. 系统故障事件，如：软硬件自身故障及其它设备设施故障等。    1. 当远程支持无法解决问题时，将派遣专业的紧急响应服务人员在第一时间到达用户单位所在地提供现场支持服务。    2. 在服务期内，故障响应时间不超过5小时，故障解决时间不超过4小时，疑难问题在8小时内给出解决方案。 | 年 | 3 |
| 3 | 应急演练 | 1. 讨论式演练：将根据选择的不同形式，最终输出应急预案、简短书面报告、草案或政策。 2. 操作式演练：将根据选择的不同形式，最终输出应急预案、正式的书面报告。 | 次 | 3 |
| 4 | 安全培训 | 1. 信息安全基础知识 2. 边界安全、传输安全、内网安全的知识培训 3. 针对评估结果和安全加固建议的培训讲解 4. 日常安全运维规范培训 5. 一般故障解决方法培训 6. 故障分析培训 7. 安全突发事件应急处理培训 | 次 | 6 |
| 5 | 防病毒建设 | 建设具有统一的、集中的、智能的和自动化的病毒防护工具，包括客户端自动化的安装、维护、配置、病毒定义码和扫描引擎的升级、定时调度、实时防护等。并采用先进的防病毒技术，能够有效的查杀各种多态病毒和未知病毒，提供三年病毒库升级服务。 | 点 | 5000 |