**第六章　项目采购需求**

### 一、招标内容

信息安全服务项目的招标内容包括安全驻点、安全评估、安全运维、安全设备维保、安全培训等信息安全服务。

**1、项目背景**

近年来，网络安全的风险日益加大，国家和企业都对防范网络安全风险非常重视。2017年6月1日开始施行的《中华人民共和国网络安全法》明确要求，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

目前，国家税务总局深圳市税务局（以下简称深圳市税务局）已经建立起一个立体交叉、覆盖面广的现代综合税收信息网络，实现了深圳市税务局与各区分局、税务系统、国库、银行的联网和无纸化办公，信息系统数量较多，包括金税三期、门户网站、电子税务局、办公自动化等等。深圳市税务局信息系统已经覆盖了所有税收征管业务和日常管理工作，信息系统的运行状况直接影响着税务机关的纳税服务水平、办事效率和社会形象。因此，信息系统的安全性、稳定性和可用性是确保高效运行的关键。

在此之前，深圳市税务局通过社会公开招标的方式，采购了专业的信息安全服务，有效地防范不同时期的病毒和黑客入侵，及时地发现和修复系统安全漏洞，确保信息系统安全、稳定和高效运行等方面，发挥了重要作用。

为了促进我局信息安全保障工作的进一步完善和提高，保证我局税务信息系统的安全可靠运行，我们将继续在“公开、公平、公正”的前提下，通过社会公开招标的方式，采购专业的信息安全服务，为我局的网络与信息安全保驾护航。

**2、项目目标**

通过信息安全服务项目，我们期望达到以下目标：

（一）完善信息安全管理体系。不断改进提升深圳市税务局的信息安全目标、战略和策略，夯实IT安全基础，完善安全措施，确保安全防护体系的有效性。适应信息安全等级保护制度要求。

（二）建立风险评估和整改机制。信息安全风险评估可以促使我们准确认识信息安全方面存在的隐患，帮助我们科学地制定信息安全工作的具体目标。按照总局要求，把风险评估工作作为一项大事来抓，建立风险评估管理制度，并按照“严密组织、规范操作、讲求科学、注重实效”的原则积极推进。根据风险评估中发现的安全隐患，制定整改措施。定期进行风险评估，运用技术评估、渗透测试等技术，发现技术、管理、人员、策略风险，提出风险处置计划，不断完善信息安全管理体系。

（三）加强日常安全运维工作，完善安全应急响应机制。安全运维工作包括安全监控、安全漏洞扫描、安全加固、防病毒管理、安全设备维护、安全事件应急响应等方面，我们需要将工作日常化、制度化和规范化，及时发现并消除信息系统中的安全隐患，确保信息系统安全运行。同时通过建立应急响应体系，完善合理的应急流程，加强安全演练，提高重大安全事件应急响应能力，快速恢复系统运行，降低安全事件造成的损失和影响。

（四）加强与税务局相关工作人员的沟通和交流，积极主动地了解和掌握应用层、网络层以及系统层的状况，将安全服务由被动地处理事件向主动地防御风险转变。

（五）建立安全培训体制和加强信息安全宣传。通过多种渠道加强有关信息安全管理制度、安全意识、安全技能宣传，建立深圳市税务局信息安全文化，确保信息安全策略、规章制度和技术规范的顺利执行，从而最大限度地降低和消除安全风险。

**3、项目范围**

我局信息安全相关的重要设备情况见下表，这些设备也是本项目的服务范围：

|  |  |  |
| --- | --- | --- |
| 序号 | 类型 | 数量 |
| 1 | 服务器 | 1364 |
| 2 | 核心网络设备 | 224 |
| 3 | 信息安全设备和系统 | 200 |
| Pc终端(含自助终端) | | 12000 |
| 合计 | | 13788 |

其中，服务器操作系统主要有AIX、Linux、Windows系列，数据库有ORACLE、SYBASE、SQL Server，中间件有WEBLOGIC，服务器品牌主要有IBM、HP、联想、曙光、浪潮、金赋等；

核心网络设备主要是华为、华三、迈普和思科的产品；

信息安全设备和系统主要有防火墙、IPS、IDS、WAF、防病毒网关、上网行为管理、桌面安全管理、网络准入、防病毒、病毒预警、防DDOS攻击和安全监控中心等系统。

### 二、项目需求

### 1、安全驻点服务要求

为减轻我局的维护成本和安全管理人员的工作压力，要求服务方安排至少两名专业安全技术人员现场值守，一名专职负责本项目的项目经理，以及在必要的时候提供安全专家的技术支持，提供信息安全日常监控维护、安全应急响应、安全通告和预警、安全咨询、安全加固和配置优化等服务，在我局安全管理人员的指导和管理下，对整个安全防护体系进行监控，对日常运行中发现的问题提出解决方案并及时处理，每月提交安全驻点服务工作情况报告。

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求** | **具体内容** |
| 1 | 服务方式 | 现场驻点和远程技术支持相结合 |
| 2 | 服务时间 | 正常上班时间和根据工作需要的非上班时间（如节假日、应急响应、加班等） |
| 3 | 服务人员 | 至少2名安全技术人员现场值守，1名项目经理专职负责本项目且每月至少提供5天的现场工作服务，1名安全专家后台提供技术支持必要的时候1小时内到场且需根据招标方要求提供至少30天/年现场工作服务  所有服务人员必须具备良好的沟通能力、协调能力和服务态度，并具备较好的口头表达和书面表达能力。 |
| 4 | 人员更换 | 服务人员的更换需经招标方同意，且更换后的服务人员资质和工作经验应达到或不低于被更换人员。若服务人员的工作能力和服务水平达不到招标方要求，招标方有权要求更换，中标方需在一个月内响应并更换为符合招标方要求的人员。 |

**1.1、安全应急服务**

安全事件是指计算机和网络设备系统的硬件、软件、数据因病毒感染或恶意攻击等安全原因遭到破坏、更改、泄漏，造成信息系统不能正常访问，或已经发现的有可能造成上述现象的安全隐患，如非授权访问、信息泄密、系统性能严重下降、网络拥塞、病毒爆发等。当出现以上安全事件时，服务方必须及时进行响应，具体要求如下：

|  |  |  |
| --- | --- | --- |
| **序号** | **要求** | **具体内容** |
| 1 | 服务要求 | 1、接到深圳市税务局通知后，现场驻点人员必须立即到场（在现场驻点人员确认无法在2小时内解决的情况下，服务方安全专家必须在1小时内到场）。处理事件并提交书面的安全事件调查分析报告：包括事故原因、过程描述、入侵来源、证据报告、解决方案、处理结果、改进建议等；从接到深圳市税务局通知起，服务方必须在24小时内解决安全事件。  2、通过建立应急响应体系，完善应急响应流程，快速对安全事件进行准确定位，及时响应处理，快速恢复系统运行，降低安全事件造成的损失和影响。  3、制订和完善重要信息安全设备和安全系统的应急响应预案，协助制定和完善重要信息系统的应急响应预案，配合深圳市税务局，根据应急预案，按照应急响应流程，组织相关人员进行应急演练，达到提高应急处理速度，多方协调联动能力，熟悉应急流程的目的。  4、如遇到特殊敏感时期需要加强安全防护，中标方必须提供有针对性的经招标方认可的安全工具和安全专家驻现场技术支持。 |
| 2 | 服务次数 | 服务期内无限次 |
| 3 | 其它要求 | 如服务方不能在规定的时间内解决问题，应及时寻求相关厂商的技术服务或外部资源进行解决。 |

**1.2、安全通告和预警服务**

定期通过邮件或移动介质等方式向我局提供信息系统相关的安全通告，包括最新出现的安全漏洞和安全警告、安全升级通告和厂商安全通告（包括但不限于Windows、AIX、Linux、Oracle、Cisco、华为、H3C、Checkpoint、天融信、绿盟、启明星辰、安恒、网神等），说明各种通告对客户信息系统的影响程度，并提出相应的解决方案。

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求** | **具体内容** |
| 1 | 服务要求 | 接到服务要求后，提供中文版本国内外厂家、著名安全组织最新发布的安全漏洞和告警、本项目相关的IT厂商发布的安全升级通告等，并说明对客户的影响程度，提出相应的解决方案。特别对深圳市税务局信息系统相关的安全漏洞和威胁进行确认和验证，对相关系统提出针对性的处理建议。 |
| 2 | 服务次数 | 服务期间无限次 |
| 3 | 服务方式 | 邮件或移动介质 |

**1.3、安全咨询服务**

安全咨询服务主要包括以下内容：

* 当系统出现异常，怀疑为安全事件时，提供事件分析和加固建议，以及安全事件追踪与取证技术支持。
* 安全体系建设和运维中，对于安全产品、安全技术、管理制度、国家法规、行业政策等问题，提供安全咨询建议和方案。
* 在信息系统开发的需求分析阶段，对系统安全风险和安全需求进行分析。
* 补充完善深圳市税务局的信息安全策略体系，根据需要制定安全管理制度和流程。
* 按照《信息安全等级保护管理办法》工作要求，协助深圳市税务局进行关键信息系统的等级保护测评和整改工作。

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求** | **具体内容** |
| 1 | 服务要求 | 接到我局咨询电话或邮件后，服务方应在2小时内提供实质性服务建议或解决方案，一个月给甲方提交一次当月咨询情况汇总报告 |
| 2 | 服务次数 | 服务期间无限次 |
| 3 | 服务方式 | 电话、传真、电子邮件等方式 |

**1.4、安全宣传服务**

协助深圳市税务局制订相关的信息安全动态月报、宣传稿件和相关课题研究等。

|  |  |  |
| --- | --- | --- |
| **序号** | **要求** | **具体内容** |
| 1 | 服务要求 | （1）每月编制一期深圳市税务局信息安全动态月报，包括当月的信息系统安全运行情况、安全形势综合分析、安全工作重点及进展、最新信息安全技术等内容。  （2）协助编写信息安全宣传文章、幻灯片、短信、海报、Flash等内容，并负责印刷张贴。  （3）参与信息安全相关的课题研究。 |

**1.5、补丁管理服务**

根据深圳市税务局《信息系统补丁管理工作规程》，服务方负责补丁跟进、补丁分级和提出补丁修复建议，要求提供从正式渠道获取的补丁，并协助进行补丁测试和补丁分发。

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求** | **具体内容** |
| 1 | 服务范围 | 深圳市税务局使用的操作系统、数据库，网络设备和安全设备等 |
| 2 | 服务内容 | 获取各种相关补丁、协助管理员完成补丁测试(包括补丁安装测试、补丁功能性测试、补丁兼容性测试和补丁回退测试)、协助管理员制订补丁加载方案，并验证监督补丁加载情况。 |
| 3 | 服务要求 | （1）补丁必须从官方或正式渠道获取；  （2）要求提交《补丁测试报告》，报告中必须包括补丁验证方法。 |
| 4 | 服务方式 | 现场服务，补丁交付通过文件上传或移动介质方式 |

**1.6、安全监控服务**

协助深圳市税务局进行信息安全日常监控，对日常运行中发现的问题提出解决方案并及时处理。

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求** | **具体内容** |
| 1 | 服务内容 | 1、利用深圳市税务局的信息安全相关设备和监控平台，为深圳市税务局提供“7x24”安全监控服务，对重要的网站页面提供实时的监控和安全事件告警。针对网页挂马、敏感内容、网页篡改、性能问题等事件，第一时间通知深圳市税务局并及时跟进处理；  2、利用深圳市税务局的日志收集系统，每个月对安全日志数据进行分析，形成审计报告。 |
| 2 | 服务方式 | 远程、现场服务 |

### 2、安全评估服务要求

**2.1、风险评估服务**

风险评估是对信息系统的影响、威胁和脆弱性进行全方位评估，归纳并总结该系统所面临的安全风险，为后续的安全规划和建设提供决策依据。

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求** | **具体内容** |
| 1 | 服务范围 | 深圳市税务局内部的服务器、网络设备、安全设备、数据库、中间件等重要系统， 核心征管、门户网站、OA、银税等重要应用系统**包括所涉及的移动客户端或基于第三方平台的客户端**，以及相关制度、预案、流程等管理体系，具体评估由深圳市税务局指定。 |
| 2 | 服务方式 | 专业的风险评估队伍在服务期间现场驻点提供服务，驻点服务人员可适当予以协助，但不得影响其日常工作 |
| 3 | 服务周期 | 一年一次。 |
| 4 | 服务工具 | 服务方必须采用业界知名的、成熟的漏洞扫描工具（至少拥有Core Impact、IBM Security AppScan、Acunetix Web Vulnerability Scanner、 N-Stalker Web Application Security Scanner、HP WebInspect、绿盟极光、启明星辰天镜、安恒信息明鉴等系统和应用漏洞扫描器的两种）进行漏洞扫描，保证对目标系统无大的影响以及扫描结果的准确性和可信度。  服务方必须提供符合标准的评估调查问卷与相关表格； |
| 5 | 服务报告要求 | 每次风险评估完成后，服务方须提交完整的评估报告，详细说明安全评估过程、信息系统安全现状、现有安全措施、信息系统面临的安全威胁、发现的安全脆弱性、安全风险排序，对高风险所带来的危害进行分析并且给出安全建议。至少包括以下几个部分：  《信息系统安全现状报告》  《信息系统安全风险分析表》  《信息系统安全风险评估报告》 |
| 6 | 其它 | 要求服务方在评估过程中不能影响业务系统的正常运行，如评估过程有可能对目标系统造成严重影响，须事先知会深圳市税务局并经过深圳市税务局的书面同意才能实施，否则，将根据影响程度追究服务方的经济责任。  在评估过程中，对有可能影响业务系统正常运行的行为，服务方必须先制定应急预案，后组织实施。 |

**2.2、渗透测试服务**

渗透测试是指在获取用户授权后，通过真实模拟黑客使用的工具、分析方法来进行实际的漏洞发现和利用的安全测试方法。这种测试方法可以非常有效地发现最严重的安全漏洞，与全面的代码审计相比，其所需的时间更短，也更有效率。

由于深圳市税务局依赖关键的业务系统对内和对外提供服务，因此，通过对这些业务系统服务器进行全面准确的测试，可以及时发现系统最脆弱的环节，及时予以修复，确保系统的安全性。

在服务期间，服务方需要对深圳市税务局的关键业务系统进行渗透测试，在每次测试完成后必须提交详细的渗透测试报告。在服务期内，若临时遇有重大事件，服务方有责任和义务临时增加渗透测试服务。

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求** | **具体内容** |
| 1 | 服务范围 | 深圳市税务局内部的服务器、网络设备、安全设备、数据库等重要系统，以及核心征管、门户网站、OA、银税等重要应用系统**包括所涉及的移动客户端或基于第三方平台的客户端**，具体测试目标由深圳市税务局指定。 |
| 2 | 服务方式 | 专业的渗透测试队伍在服务期间现场驻点提供服务，驻点服务人员可适当予以协助，但不得影响其日常工作 |
| 3 | 服务周期 | （1）为深圳市税务局提供一年两次渗透测试服务，服务完成后提交详细的渗透测试报告；  （2）若临时遇有重大事件，需增加渗透测试服务，但每年增加不多于两次。 |
| 4 | 服务工具 | 服务方必须采用业界知名的、成熟的漏洞扫描工具（至少拥有Core Impact、IBM Security AppScan、Acunetix Web Vulnerability Scanner、 N-Stalker Web Application Security Scanner、HP WebInspect、绿盟极光、启明星辰天镜、安恒信息明鉴等系统和应用漏洞扫描器的两种）进行漏洞扫描，保证对目标系统无大的影响以及扫描结果的准确性和可信度。  服务方要具有实现渗透测试的技术能力，并在不影响业务系统正常运行的前提下完成渗透测试，产生相应的文档及结论。 |
| 5 | 服务报告要求 | 每次渗透测试完成之后，服务方应提供一份渗透测试报告。渗透测试报告必须详细说明渗透测试过程中发现的漏洞信息、证据，以及整体网络安全分析和安全加固建议。 |
| 6 | 其它 | 要求服务方在渗透测试过程中不能影响业务系统的正常运行，如渗透测试过程有可能对目标系统造成严重影响，须事先知会深圳市税务局并经过深圳市税务局的书面同意才能实施，否则，将根据影响程度追究服务方的经济责任。  在渗透测试过程中，对有可能影响业务系统正常运行的行为，服务方必须先制定应急预案，后组织实施。 |

**2.3、安全迎检服务**

安全迎检和整改是指根据外部信息安全检查和测评机构的检查要求，协助深圳市税务局提前进行自查，并提出整改方案，协助完成整改；在外部机构检查过程中配合检查，提供相关技术支持；针对外部机构的检查结果，编写信息安全检查汇总分析报告。

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求** | **具体内容** |
| 1 | 服务范围 | 深圳市税务局内部的服务器、网络设备、安全设备、数据库等重要系统，以及核心征管、门户网站、OA、银税等重要应用系统**包括所涉及的移动客户端或基于第三方平台的客户端**，具体工作内容由深圳市税务局指定。 |
| 2 | 服务方式 | 根据招标方工作进度安排，安排专业团队现场驻点提供服务，驻点服务人员可适当予以协助，但不得影响其日常工作 |
| 3 | 服务周期 | （1）为深圳市税务局提供一年两次迎检服务，服务完成后提交详细的自查报告；  （2）若临时遇有重大事件，需增加迎检服务，但每年增加不多于两次。 |
| 4 | 服务报告要求 | 每次迎检工作结束，编写信息安全检查汇总分析报告。报告必须详细说明检查工作中发现的问题，并提出整改建议。 |

### 3、安全运维服务要求

**3.1、安全扫描与加固服务**

在安全体系的建设和维护过程中，通过漏洞扫描，及时发现信息系统和网络及安全设备存在的各种安全隐患和漏洞，通过打补丁、增强安全配置、调整系统架构和安全策略等方式及时进行安全加固和优化，持续提高系统的安全性和抗攻击能力，将整个系统的安全状况维持在较高的水平，减少安全事件发生的可能性。

|  |  |  |
| --- | --- | --- |
| **序号** | **要求** | **具体内容** |
| 1 | 服务范围 | 对深圳市税务局所有服务器、网络设备、安全设备、数据库、应用系统及**移动客户端或基于第三方平台的客户端**进行漏洞扫描和安全加固 |
| 2 | 服务方式 | 专业的安全扫描人员在服务期间现场驻点提供服务，驻点服务人员可适当予以协助，但不得影响其日常工作 |
| 3 | 服务周期 | （1）每季度至少进行一次全面的漏洞扫描（含系统层和应用层的扫描）和安全加固；  （2）遇有重大事件、信息系统发生重大变更后或厂商发布严重安全警告时，根据深圳市税务局要求不定期进行漏洞扫描和安全加固。  (3)针对深圳市税务局的税收征管关键系统及互联网应用系统至少每月进行一次漏洞扫描和安全加固  （4）新系统上线前。 |
| 4 | 服务工具 | 服务方必须采用业界知名的、成熟的漏洞扫描工具（至少拥有Core Impact、IBM Security AppScan、Acunetix Web Vulnerability Scanner、 N-Stalker Web Application Security Scanner、HP WebInspect、绿盟极光、启明星辰天镜、安恒信息明鉴等系统和应用漏洞扫描器的两种）进行漏洞扫描，保证对目标系统无大的影响以及扫描结果的准确性和可信度。 |
| 5 | 服务报告要求 | （1）每次扫描完成后，必须提交完整的网络安全状况评估报告，采用图表等各种直观的形式说明目前系统存在的安全漏洞数量、类型、严重程度、分布范围等，以及各种漏洞的详细说明和操作性很强的解决方案（包括各种补丁和工具的下载地址，操作步骤等）；  （2）针对对外服务的信息系统，必须提交应用层安全扫描报告；  （3）必须提交本次评估结果和上次评估结果的对比分析和安全状况变化趋势报告。 |
| 6 | 其它 | 要求服务方在扫描过程中不能影响业务系统的正常运行，如扫描过程有可能对目标系统造成严重影响，须事先知会深圳市税务局并经过深圳市税务局的书面同意才能实施，否则，将根据影响程度追究服务方的经济责任。  在扫描过程中，对有可能影响业务系统正常运行的行为，服务方必须先制定应急预案，后组织实施。 |

**3.2、安全巡检与审计服务**

通过对信息系统定期进行安全检测（工具扫描及安全专家人工检测），及时发现信息系统（网络架构、网络设备、服务器主机、操作系统、数据库和用户账号、口令等安全对象）存在的各种安全隐患，提出系统加固建议。

对防火墙、入侵防御、入侵检测、WEB应用扫描、安全配置检查、防病毒软件、桌面安全管理、安全监控中心、WEB应用防火墙、防病毒网关等设备和系统进行事件审计和日志分析，检查策略是否有效，配置是否安全，是否有可疑事件发生，必要时调整安全策略。

根据我局《信息系统安全巡检工作规程》要求，每半年组织一次安全巡检，一般系统的安全巡检工作由系统管理员自行完成，服务方负责提供工具并培训系统管理员直到其可独立进行巡检。服务方负责检查核心系统和抽查一般系统。

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求** | **具体内容** |
| 1 | 服务方式 | 专业的安全审计人员在服务期间现场驻点提供服务，驻点服务人员可适当予以协助，但不得影响其日常工作 |
| 2 | 服务周期和范围 | 1. 每季度一次对核心系统（防火墙、防病毒系统、IDS、IPS、WAF、重要路由器、核心交换机、重要服务器）进行安全检查和审计； 2. 每季度一次对一般系统以抽查形式进行安全检查和审计（抽查比例20%）。 3. 每半年一次对深圳市税务局全系统进行一次全面的安全巡检。 4. 招标方将依据安全巡检结果对深圳市税务局各区分局定期进行现场巡查，投标方需根据要求负责组织深圳市税务局工作人员赴各区分局实地检查。 |
| 3 | 服务对象 | 防火墙、入侵防御、入侵检测、WEB应用扫描、安全配置检查、防病毒、桌面安全管理、安全监控中心、WEB应用防火墙、防病毒网关、防DDOS攻击等安全设备以及主要路由器、交换机和服务器。 |
| 4 | 服务要求 | 完成安全巡检和审计服务后，必须提交设备巡检报告、安全审计报告和安全策略调整建议等。 |

**3.3、应用安全开发及代码审计服务**

针对应用系统的生命周期，在系统建设及日常运维方面提供专业的咨询顾问服务，并提供源代码安全审计服务以发现应用程序编码过程中造成的安全漏洞。

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求** | **具体内容** |
| 1 | 服务要求 | 根据国家税务总局网络安全“三同步”的要求，落实应用系统和网络安全同步规划、同步建设、同步使用，将网络安全贯穿应用系统项目建设的全过程。在应用系统需求分析、方案设计、开发测试、集成部署阶段进行安全方案的审核，提供安全咨询和建议，在系统上线前进行全面的安全测评和源代码安全审计以发现安全漏洞，并提供修复建议。 |
| 2 | 服务周期 | 新系统开发、上线前 |
| 3 | 服务方式 | 现场服务 |

### 4、安全设备维保服务

负责深圳市税务局信息安全相关的安全设备、系统的全面维保服务，确保信息安全系统、设备稳定有效运行。

|  |  |  |
| --- | --- | --- |
| **序号** | **要求** | **具体内容** |
| 1 | 服务范围 | 深圳市税务局所有已过保修期的信息安全设备，包括将在服务期内过保修期的设备。 |
| 2 | 服务要求 | 针对深圳市税务局所有已过保修期和将在服务期内过保修期的安全设备进行维保服务，确保设备可用性。  中标方须在中标后至合同签订前提交原厂商向中标方提供服务的承诺函，并在合同签订后一个月内按合同服务期购买原厂维保服务。 |
| 3 | 服务内容 | 提供对所需维护对象的保修服务,其中包括硬件更换和维修、软件支持、修复性服务及预防性服务由投标方负责进行，具体内容如下：  （1）定期进行预防性检查维护；  （2）对维保设备的软硬件及操作系统的安装、调试、扩充、移机等辅助性工作；  （3）提供硬件维护服务、提供软件版本及特征库升级服务；  （4）软、硬件设备故障及时响应和修复；  （5）及时提供技术咨询，提出合理化建议；  （6）提供技术培训和相关的行业技术信息。 |
| 4 | 服务响应时间 | （1）严重问题：设备及系统无法使用和访问，导致系统的崩溃以及造成系统重要功能丧失的故障，在1小时内进行响应处理，无法及时处理应提供替代设备或方案。  （2）中等问题：设备及系统运行不稳定，系统的操作和运行不造成重要影响的问题，也包括对性能和新功能的要求，在2小时内响应处理。无法及时处理应提供替代方案。  （3）一般问题：设备及系统发生不可重现的错误报告、基本配置和功能实现的要求等，不影响设备及系统运行的各种故障情况，在7小时内进行响应处理。 |
| 5 | 服务方式 | 对严重问题及中等问题提供现场服务，对一般和其他问题可提供Email、电话等远程支持方式。 |
| 6 | 其他 | 设备出现故障并被确定需要维修时，服务方负责将故障部件返厂进行维修，设备应在7个工作日内修复；修复期间服务方应提供不低于故障设备规格型号档次的备用设备深圳市税务局使用。如有特殊情况由双方协商解决。 |

具体需维保信息安全设备如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **设备类型** | **设备厂家及型号** | **过保日期** | **数量（台/套）** | **备注** |
| 1 | 防火墙 | Checkpoint IP397 | 已过保 | 2 | 需购买原厂维保服务 |
| 2 | 防火墙 | 天融信TG-5564 | 已过保 | 2 |  |
| 3 | 防火墙 | 天融信TG-470C | 已过保 | 6 |  |
| 4 | 防火墙 | 天融信 TG-5130-GS | 已过保 | 18 |  |
| 5 | 防火墙 | 天融信 TG-50008-GS | 已过保 | 24 |  |
| 6 | 防火墙 | 天融信 TG-5628-GS | 已过保 | 4 |  |
| 7 | IDS | 启明星辰 天阗 NS2200-F | 已过保 | 9 | 需购买原厂维保服务 |
| 8 | WEB应用防火墙 | 安恒 DAS-WAF-3500 | 已过保 | 2 | 需购买原厂维保服务 |
| 9 | 防病毒网关 | 网神 SecAV3600-U020M | 已过保 | 2 | 需购买原厂维保服务 |
| 10 | 防DDOS攻击 | 绿盟 ADS NX3 | 2019年12月 | 2 | 需购买原厂维保服务 |
| 11 | IDS | 启明星辰 NT3000-PF-BRP-Y | 2019年9月 | 4 | 需购买原厂维保服务 |
| 12 | IDS | 启明星辰 NT3000-LT-S-Y | 2019年9月 | 5 | 需购买原厂维保服务 |
| 13 | IGuard | 上海天存 | 2019年11月 | 1 |  |
| 14 | IPS | 天融信 | 2019年8月 | 1 | 需购买原厂维保服务 |
| 15 | 扫描系统 | 天镜脆弱性扫描与管理系统 | 2019年6月 | 1 | 需购买原厂维保服务 |
| 16 | 扫描系统 | 绿盟RSAS NX3 | 2019年6月 | 1 | 需购买原厂维保服务 |

### 5、安全培训服务要求

**5.1、安全技能培训**

安全管理工作离不开全体用户的参与和专业安全技术人员的执行，为加强深圳市税务局计算机用户和维护人员的安全意识和技能，服务方需提供安全技能培训服务，培训内容须包括但不限于以下内容：

* 常见攻击方式介绍与案例分析
* UNIX/WINDOWS系统安全配置和管理
* 常用安全工具
* 网络设备安全建议
* 国内外信息安全管理标准和体系介绍
* IDS、IPS、安全审计、DDOS等流行安全技术和产品介绍
* 安全事件应急处理与分析
* 风险评估培训
* 等级保护培训

具体要求如下：

|  |  |  |
| --- | --- | --- |
| **序号** | **要求** | **具体内容** |
| 1 | 服务要求 | （1）全年组织一次技术培训班，授课时间为5天，培训对象为深圳市税务局指定人员（不多于50人）；  （2）培训讲师具备ISO27001 LA、CISP、CISSP、CISI其中一种安全认证资质；  （3）培训前提供电子版教材给深圳市税务局。  （4）培训的师资、交通、场地、食宿等由中标方负责落实。 |
| 2 | 服务方式 | 现场讲座 |

**5.2、安全意识培训**

面向深圳市税务局的全体工作人员，目的是提高整个深圳市税务局普通计算机使用人员的安全意识和安全防护能力，使用户充分了解既定的安全策略。该培训力图改变用户对信息安全的态度，使普通的计算机使用人员知晓信息安全的重要性、安全管理制度的要求及其职责范围内需要注意的安全问题。

每年对深圳市税务局全体工作人员进行一次安全意识培训，内容涵盖信息安全的基本概念、安全管理制度要求、日常操作安全须知、常见应用软件安全配置、恶意代码的防范等知识。

|  |  |  |
| --- | --- | --- |
| **序号** | **要求** | **具体内容** |
| 1 | 服务要求 | 培训对象：深圳市税务局全体人员  （1）一年一次；  （2）培训讲师具备ISO27001 LA、CISP、CISSP、CISI其中一种安全认证资质；  （3）培训前提供电子版教材给深圳市税务局并进行试讲。  （4）定期制作信息安全相关电子课件，通过各种方式发送全局人员进行信息安全宣传教育 |
| 2 | 服务方式 | 培训地点由深圳市税务局提供。中标方指派讲师赴各区分局进行现场讲座，每次讲座时长2小时。 |