**询价文件**

网络安全运维服务项目采购需求

**一、项目概况**

1、项目名称

黄石市住房公积金中心网络安全运维服务项目

2、项目背景

2017年6月1日，《中华人民共和国网络安全法》正式颁布施行，明确要求对关键信息基础设施实行重点保护。规定“应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”，“建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用”。

2017年7月11日，《关键信息基础设施安全保护条例(征求意见稿)》正式公布征求意见，从支持与保障、关键信息基础设施范围、运营者安全保护、产品和服务安全、监测预警、应急处置和检测评估、法律责任等诸多方面，对于关键信息基础设施保护相关的一系列制度要素作了更为具体的规定。

黄石市住房公积金中心部署大量的信息资产，信息系统群庞大，信息安全管理层面复杂。因此，需要充分考虑可能面临的各类安全风险，建立健全网络安全管理机制和完善的信息安全管理体系，指导和监督安全建设和运维过程中对风险的控制，以确保信息系统安全、稳定、高效的运行。

本项目通过采购第三方的网络与信息安全保障服务，确保客户在服务期内加强网络安全整体保障，提升网络安全防护水平，严格排查安全漏洞隐患，不发生重大网络安全和信息安全事件，各类信息系统和网络安全正常运行，目标系统得到有效保护。

3、服务范围

本次保障范围涉黄石市住房公积金中心单位网络安全。

4、服务目标

总体目标：提升安全管理水平、补强安全“短板”、提高网络安全事件应急恢复能力，努力实现安全防护水平由被动防御到主动发现的转变，做到网络与信息安全态势可感知、安全事件可预警。

5、服务周期

自合同签订生效日起算两年服务期。

**二、网络安全运维服务内容**

（一）安全巡检服务

1、服务内容

安全巡检作为主动运维的一种手段，将主动发现安全隐患来代替被动解决安全问题，极大的提高信息系统的安全防护水平。

定期对客户信息系统中包括安全设备进行全面地安全巡检，主要内容包括安全设备状态检查、安全设备配置检查、设备升级更新等。

2、服务周期

安全巡检服务周期每月1次，一年12次。

3、成果交付

定期提供安全设备巡检服务，在项目实施过程中，提交完整的阶段交付物，交付物包括但不限于以下文档：

《安全设备巡检报告》。

（二）重保值守服务

1、服务内容

重保期间，为能及时对监测到的各种告警信息进行分析，出现异常事件及时决策和处置，将派遣具有丰富的入侵分析和应急处置经验的高级安全专家进行现场5\*8值守。

通过对相关事件告警信息进行分析，提供抑制手段，入侵威胁清除，排查攻击路径，恶意文件清除，还原攻击路径，分析入侵事件原因，结合现有安全防御体系，进行指导安全加固、提供整改建议、防止重保期间出现安全事件。

现场安全值守工作主要包括如下方面工作：

1）、安全设备日常监控

安全设备健康情况实时监控，包含：CPU使用率、内存占用率、接口流量、接口工作状态、硬盘使用情况等设备健康相关的基本参数监控。

安全设备告警事件实时监控，包含：拒绝服务攻击，网络病毒爆发，漏洞远程利用、恶意代码传递等高危事件告警信息。

2）、安全事件协助处理

当安全设备产生高危事件报警时，信息安全专家将积极协助用户相关人员对报警事件进行确定、排查、分析和处理。

2、服务周期

重保值守服务每年保障不少于3次。

3、服务交付

专家值守服务，交付物包括但不仅限于以下文档：

《专家值守报告》

（三）安全培训服务

1、服务内容

针对根据不同的用户类型安排有针对性的培训内容。

技术人员主要包括：操作人员、开发人员、维护人员等。

培训目标：面向专业技术人员，以提升网络安全专业人员技术水平为目的，讲解网络威胁的种类、常见黑客攻击手法思路、安全防护方案及日常错误等。

全员培训主要包括：安全意识培训等。

培训目标：面向普通员工，讲解当前网络环境中存在的常见威胁、网络攻击手法、存在的风险，提升普通员工在日常工作、生活中网络安全防护意识，让安全事故可以得到有效的避免。

课程体系、内容不限于：

信息安全基础培训，提供最基础的信息安全名词、知识点、相关产品、保障措施、安全意识等培训。

信息安全管理体系培训，信息系统的整个生命周期中，从技术、工程、管理和人员各个方面的安全保障要求，确保信息的保密性、完整性和可用性特征，实现和贯彻组织机构策略，并将风险降低到可接受的程度，以保护组织机构信息系统资产。

安全攻防培训，针对各类网络攻击及对应的安全防护措施思路进行培训。帮助用户了解黑客实施攻击的思维和行为模式，同时关注网络、操作系统、应用系统的各种典型漏洞和问题，并利用典型案例的分析来理解黑客发掘漏洞展开攻击的实际过程。针对具体漏洞和攻击手段，提出相应的防护策略和解决方案。

网络安全产品培训,针对主流的信息全线网络安全软件产品，提供技术培训，包括：安全管理平台、日志审计平台、网络数据库审计平台、终端管理平台等。

2、服务周期

安全培训宣贯服务每年2次，每次邀请专家不少于0.5天的培训课程。

3、主要交付物

在项目实施过程中，提交完整的阶段交付物，交付物包括但不限于以下文档：

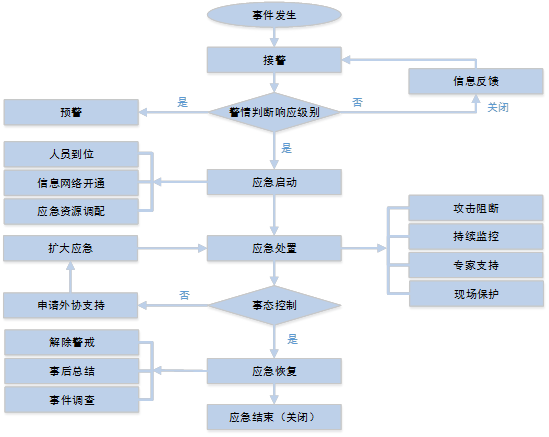
《网络安全培训》PPT等文档。

（四）应急响应服务

1、服务内容

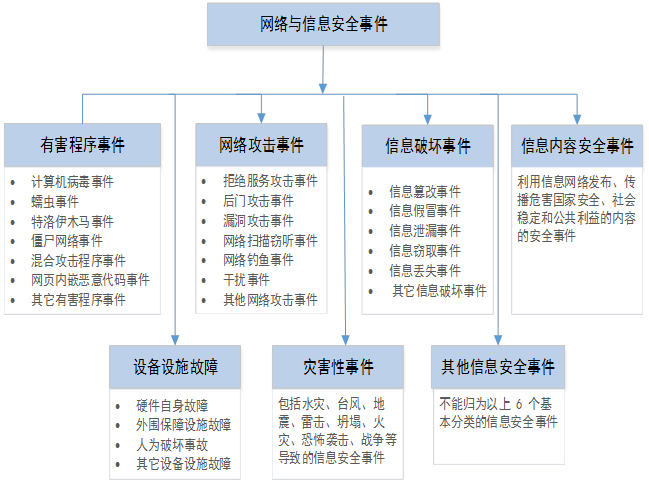
当信息系统遇到突发的安全问题如：发生网络入侵事件、大规模病毒爆发、遭受拒绝服务攻击等，保障在30分钟内进行有效响应，2小时内应急响应人员到现场进行应急，对现场发现的脆弱性立刻加固，防止被入侵成功。对已产生的安全事件启动应急措施，确定安全事件的威胁和破坏的严重程度，事件进行抑制和溯源分析，找到脆弱点，进行加固并上报。

在安全事件发生之后，应急响应整体工作流程如下图所示：



应急处置流程

根据GB/Z 20986 2007《信息安全技术信息安全事件分类分级指南》对信息安全事件分类的分类方法，综合考虑客户系统网络与信息化建设的具体情况，客户系统网络与信息安全事件的专项应急预案可归类分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件等7个基本分类。



网络与信息安全事件分类

2、服务周期

应急响应服务按需每年提供不少于20人天的现场应急服务。

3、成果交付

在项目实施过程中，提交完整的阶段交付物，交付物包括但不限于以下文档：

《应急响应报告》

（五）网络安全评估及协助加固服务

1、服务内容

**漏洞扫描**

采用具有自主知识产权的漏洞扫描工具对服务范围内的业务系统主机、应用、数据库进行专业的漏洞扫描，并人工验证所发现的web应用漏洞、主机操作系统漏洞、数据库漏洞、逻辑缺陷、弱口令、信息泄露及配置不当等脆弱性问题。

**回归测试**

在用户修改了高危代码或漏洞后，将重新进行安全测试来确认修改没有引入新的错误或导致其他代码产生错误；在正式进行回归测试前，需确定回归测试的对象与范围，依靠自动化漏洞扫描及人工检查等技术手段配合验证，回归测试也有效提高了整改和加固措施的有效性，大幅降低系统测试、维护升级等阶段的成本。回归测试作为软件生命周期的一个组成部分，在渐进和快速迭代中回归测试策略运用比较频繁，要求投标人通过合理的技术手段降低未加固漏洞的安全风险，提升信息系统安全加固的有效性。

**安全协助加固**

根据安全检测服务结果，高级安全专家针对所发现的安全漏洞及安全风险，提出可操作性强、效果佳的整改建议，并协助用户完成整改。

网络安全加固主要从以下几个方面考虑：

**服务器系统主要从以下方面进行安全加固和优化：**

安全补丁的选择性安装；

最小服务原则的贯彻，禁用不必要系统服务；

最小授权原则的贯彻，细化授权原则；

SSH管理数据加密配置；

账号、密码安全策略；

文件、目录访问控制；

关键系统服务安全配置；

安全日志策略。

**数据库系统主要从以下方面进行安全加固和优化：**

安全补丁的选择性安装；

最小服务原则的贯彻，禁用不必要的服务模块；

最小授权原则的贯彻，细化用户访问不同数据库、数据表的授权原则；

数据库系统默认账号的禁用或调整；

数据库系统账号、密码安全策略；

数据库系统认证和审核策略配置；

MS SQL Server扩展存储过程的调整；

MS SQL Server注册表访问过程的调整；

MS SQL Server缓冲区溢出漏洞的安全加固；

Oracle缓冲区溢出隐患的安全加固。

**应用系统主要从以下方面进行安全加固和优化：**

安全补丁的选择性安装；

最小服务原则的贯彻，禁用不必要的服务模块；

最小授权原则的贯彻，尽量削弱应用系统服务的运行权限；

IIS的针对性安全加固和优化；

Tomcat的安全加固和优化；

WebLogic的针对性安全加固和优化；

Foxmail的针对性安全加固和优化。

**网络设备安全和网络安全防护策略优化加固：**

Internet、Intranet和Extranet之间及它们内部各VLAN或区域之间边界划分是否合理；

在网络节点（如路由器、交换机、防火墙等设备）互连互通应根据实际需求进行严格控制；

验证设备当前配置的有效策略是否符合组织确定的安全策略。

2、服务周期

协助加固服务周期每季度1次，一年4次。

3、成果输出

交付物包括但不仅限于以下文档：

《安全评估报告》、《安全整改报告》

（六）配合上级部门检查服务

1、服务内容

配合中心进行上级部门安全检查，协助安全检查资料收集、整理、并根据实际需求填写安全检查报告及填报对应检查系统，并最后完成对应总结报告。2、服务周期

按照监管单位需求，配合完成检查。

3、成果输出

交付物包括但不仅限于以下文档：

《安全检查报告》

**三、网络安全运维服务清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务描述 | 服务内容 | 参数描述 |
| 1 | 安全巡检服务 | 服务内容 | 定期对客户信息系统中包括安全设备进行全面地安全巡检，主要内容包括安全设备状态检查、安全设备配置检查、设备升级更新等。 |
| 服务周期 | 每月1次，一年12次。提供两年服务 |
| 2 | 重保值守服务 | 服务内容 | 在重要活动或关键时期，按要求派遣经验丰富的安全人员，提供现场安全保障和安全值守，按需完成每日保障支持、安全监控以及损失评估、外部攻击源追溯，内部脆弱性分析等应急处置任务。 |
| 服务周期 | 每年保障至少3次。提供两年服务 |
| 3 | 安全培训服务 | 服务内容 | 针对相关管理人员和技术人员进行安全意识、安全管理以及安全事件应急处置培训服务，提升网络安全方面的处置能力。。 |
| 服务周期 | 每年至少2次。提供两年服务 |
| 4 | 应急响应服务 | 服务内容 | 提供7\*24小时现场专业应急响应服务，当安全威胁事件发生后迅速采取的措施和行动，以最快的速度恢复系统的可用性，阻止和降低安全威胁事件带来的严重性影响。 |
| 服务周期 | 每年按需提供不少于20人天的现场应急服务，提供两年服务 |
| 5 | 网络安全评估及协助加固服务 | 服务内容 | 服务人员使用商用安全评估工具对评估目标范围内对象进行漏洞扫描，并人工验证所发现的web应用漏洞、主机操作系统漏洞、数据库漏洞、逻辑缺陷、弱口令、信息泄露及配置不当等脆弱性问题。 根据安全评估结果的具体情况，协助客户制定服务目标的加固建议，针对不同类型的目标系统，通过打补丁、修改安全配置、增加安全机制、建议添置安全设备等方法，合理加强服务目标的安全性。 |
| 服务周期 | 每季度1次，提供两年服务 |
| 6 | 配合上级部门检查 | 服务内容 | 配合中心进行上级部门安全检查，协助安全检查资料收集、整理、并根据实际需求填写安全检查报告及填报对应检查系统，并最后完成对应总结报告。 |
| 服务周期 | 提供两年服务 |

**附件一：**

**报 价 函**

报价文件请各供应商自拟。

日期： 年 月 日

**法人代表授权书**

（采购人）：

兹授权 同志为我公司参加贵单位组织的网络安全运维服务项目采购询价活动的授权代表人，全权代表我公司处理在该项目活动中的一切事宜。

代理期限从 年 月 日起至 年 月 日止。

供应商： （加盖公章）

法定代表人： （签字）

签发日期： 年 月 日

附：代理人工作单位：

职务： 性别：

身份证号码：

|  |
| --- |
| 被授权人身份证复印件 |

**其他证明文件、资料等**

1、公司营业执照

2、相关资质证书

以上文件均为复印件并加盖公章