互联网新技术新业务

信息安全评估报告

业务名称：乐山社保查询系统

2017年8月28日

中国移动通信集团四川省公司

1. 业务基本情况介绍
   1. 业务名称

乐山社保查询系统

* 1. 业务功能介绍

1、乐山社保用户可以登录系统，亦可以注册，或者下载终端App

2、用户基本信息查询

3、参保信息查询

4、医院账户查询

5、缴费信息查询

6、待遇信息查询

* 1. 技术实现方式介绍

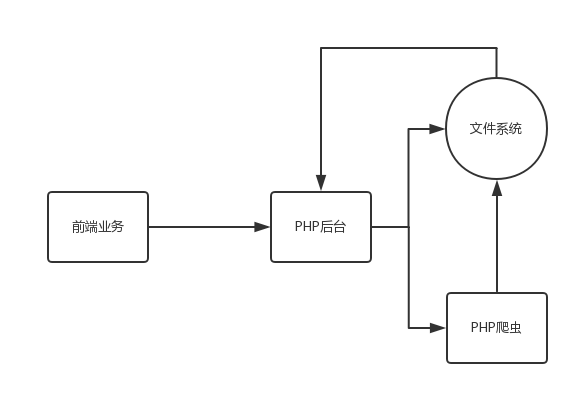
1、使用PHP 爬虫，获取乐山门户网站的社保信息

2、使用PHP搭建Web后台网站，实现后台业务逻辑

3、使用Bootstrap和jQuery实现前端界面设计

4、使用文件存储，作为中间信号通信

* + 1. 业务网络结构



* + 1. 业务订购/退订流程
    2. 主要功能实现流程
  1. 用户及市场情况

1. 安全评估情况
   1. 安全评估情况概述
   2. 评估人员组成
   3. 评估实施流程
   4. 评估结果
      1. 业务应用安全

|  |  |  |  |
| --- | --- | --- | --- |
| **评分点** | **指标** | **评估意见** | **研判依据** |
| 用户 | 用户规模 |  |  |
| 用户类型 |  |  |
| 用户相关性 |  |  |
| 用户身份信息真实性 |  |  |
| 用户身份信息保护 |  |  |
| 信息内容 | 信息内容可审核性 |  |  |
| 信息内容多样性 |  |  |
| 信息内容相关性 |  |  |
| 信息载体 | 信息呈现方式 |  |  |
| 语言类型 |  |  |
| 信息生成 | 信息源 |  |  |
| 信息产生方式 |  |  |
| 信息传播 | 信息传播方式 |  |  |
| 通信媒介 |  |  |
| 信息传递实时性 |  |  |
| 信息接收 | 信息收取方式 |  |  |
| 信息留存 | 用户留存使用日志记录 |  |  |

* + 1. 业务平台安全

|  |  |  |  |
| --- | --- | --- | --- |
| **评分点** | **指标** | **评估意见** | **研判依据** |
| 设备位置分布 | 服务器、机房或节点的地理位置分布 |  |  |
| 资源调度方式 | 资源调度方式 |  |  |
| 业务合作 | 合作方式的合规性 |  |  |
| 合作企业的安全能力 |  |  |
| 开放接口 | 是否提供第三方API接口 |  |  |

* + 1. 业务规范安全

|  |  |  |  |
| --- | --- | --- | --- |
| **评分点** | **指标** | **评估意见** | **研判依据** |
| 用户信息管理 | 用户信息泄露风险 |  | *备注：一旦用户个人信息保护不力发生泄漏，则可能导致相关精准个人信息被诈骗份子利用进而实施精准诈骗，此项的研判依据是企业具备哪些用户个人信息保护管理机制和技术措施* |
| 业务逻辑安全 | 业务逻辑漏洞风险 |  | *备注：以一卡多号、短信营业厅、网上营业厅等未代表的电信业务在业务模式、机制流程等方面存在的安全漏洞，如业务流程不完善、未实施二次确认机制、短信验证码下发环节用户安全提醒不完善、业务登录提示不足等，有可能被诈骗份子利用设计各种诈骗场景脚本、冒充用户实施诈骗。此项的研判依据是企业对以上业务在业务模式、机制流程等方面配套了哪些管控措施业务逻辑漏洞检测机制和和相应应急措施* |
| 通讯信息管理 | 基础电信业务的诈骗电话、诈骗短信传播风险 |  | *备注：对于电话卡、语音专线、数据专线短信端口、400、一号通、商务总机、融合通信等基础电信业务，如果企业事前、事中业务规范管理存在漏洞或技术管控手段建设不足，如违规为个人用户办理业务、用户资质审核不严、代理渠道管理薄弱、语音专线未实施主叫鉴权或呼叫转移管控不力、外呼管理不严、业务落地号码管理薄弱、业务使用复核监测不足、异常行为用户监测管控、不良呼叫号码监测处置能力不足等，则相关电信线路、业务资源极有可能被诈骗份子获取和利用，产生违法使用、违规外呼、呼叫频次异常、私自改变业务使用用途等违法违规业务使用行为，通过利用改号软件修改主叫号码、设置主叫号码为空号或禁显、利用真实号码拨打电话、发送短信等具体通讯联络方式实施电话诈骗、短信诈骗。此项的研判依据是企业针对上述业务，企业在事前、事中业务规范管理方面，配套了上述哪些管理手段，是否还存在规范管理漏洞；在技术管控手段建设方面，配套了上述哪些技术管控手段，是否还存在手段建设不足* |
| 互联网业务的通讯信息诈骗违法信息传播风险 |  | *备注：即时通信、搜索引擎、手机应用、软件商城、电商平台、社交平台、网站页面等互联网业务，有可能成为不法分子进行个人信息贩卖、获取诈骗实施软件和工具（改号软件、诈骗脚本写作方法、非法买卖电话卡、买卖银行卡、身份证识别设备破解软件、虚拟交易软件、相关木马病毒等）、雇佣人员（写作诈骗脚本、发送伪基站信息、拨打电话、转账取款、专业洗钱等）、交流教唆通讯信息诈骗等的渠道途径。此项研判依据是企业针对上述违法信息的发布、传播等，在审核、监测、阻断等环节配套了哪些管理和技术管控手段*。 |
| 追踪溯源风险 |  | *备注*：*若存在落实电话用户实名登记不力、业务资质审核不严、未有效留存日志信息等问题，则会加大通讯信息诈骗调查取证、事后溯源工作难度。此项侧研判依据是从用户实名登记、业务资质审核、日志留存等方面的落实情况，评判追踪溯源能力* |

* 1. 评估整改和复核落实
     1. 整改情况

|  |  |  |  |
| --- | --- | --- | --- |
| **编号** | **安全风险** | **风险等级** | **整改情况** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |

* + 1. 高危风险备案

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **编号** | **残留风险** | **风险等级** | **风险描述** | **控制措施** | **责任声明** | **责任人签字/盖章** |
| 1 |  |  |  |  |  |  |

1. 配套安全管理措施
   1. 日常安全管理介绍
      1. 定期开展信息安全评估
      2. 违法信息监测
      3. 投诉处置机制
      4. 日志留存溯源
      5. 安全管控
   2. 应急管理措施介绍
   3. 企业保障能力评估
      1. 业务应用安全及业务平台安全保障能力评估

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **检查分类** | | | **检查指标** | **检查结果** | **研判依据** | **证明材料** |
| 业务应用安全保障基线要求 | 用户管理 | 普通账号身份验证 | 注册环节是否进行个人真实信息验证 | 符合[]  不符合[ ]  不涉及[] |  |  |
| 是否具备管控违规注册信息的管理措施 | 符合[]  不符合[ ]  不涉及[] |  |  |
| 公众账号身份验证 | 注册环节是否进行公众账号真实信息验证 | 符合[]  不符合[ ]  不涉及[] |  |  |
| 注册信息审核 | 是否具有用户注册相关规定告知提示 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 是否具有对用户注册信息的审核机制 | 符合[] 不符合[ ]  不涉及[ ] |  |  |
| 用户账号分级管理 | 是否建立账户差异化违法信息发布安全等级机制 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 用户投诉管理 | 是否公示用户举报投诉途径 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 信息内容管理 | | 是否建立对违法违规内容发布有效识别手段及处置策略 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 是否建立违法信息样本库 | 符合[ ]  不符合[]  不涉及[] |  |  |
| 信息搜索功能管理 | | 是否建立有效手段隔离违法违规信息检索内容 | 符合[ ]  不符合[ ]  不涉及[] |  |  |
| 信息发布递送功能管理 | | 是否建立公众账号内容发布监测机制 | 符合[ ]  不符合[ ]  不涉及[] |  |  |
| 信息社区平台功能管理 | | 是否建立社区平台信息转发评论监测机制 | 符合[ ]  不符合[ ]  不涉及[] |  |  |
| 应用分发平台功能管理 | 应用开发者管理 | 是否具有应用开发者资质审核管理措施 | 符合[ ]  不符合[ ]  不涉及[ ] |  |  |
| 是否在协议中明确应用开发者的安全责任 | 符合[]  不符合[ ]  不涉及[] |  |  |
| 是否建立应用开发者违规记录档案 | 符合[]  不符合[ ]  不涉及[] |  |  |
| 应用安全审查 | 是否对应用进行上线前安全审查 | 符合[]  不符合[ ]  不涉及[] |  |  |
| 日常监测 | 是否对应用进行日常监测 | 符合[]  不符合[ ]  不涉及[] |  |  |
| 违法应用处置 | 是否建立有效的违规应用下架处理机制 | 符合[]  不符合[ ]  不涉及[] |  |  |
| 信息即时交互功能管理 | 群组功能管理 | 是否设置群组人数上限 | 符合[ ]  不符合[ ]  不涉及[] |  |  |
| 是否告知群组功能申请人的安全责任 | 符合[ ]  不符合[ ]  不涉及[] |  |  |
| 匿名发布功能管理 | 是否具有“前台匿名、后台实名”的技术手段 | 符合[]  不符合[ ]  不涉及[] |  |  |
| 转发功能管理 | 是否具有针对用户安全级别管控用户信息操作权限的技术手段 | 符合[ ]  不符合[ ]  不涉及[] |  |  |
| 信息销毁功能管理 | 是否具备恢复已销毁信息的技术手段 | 符合[ ]  不符合[ ]  不涉及[] |  |  |
| 安全规则张贴与主动提示 | | 是否全程明确告知提示用户禁止发布、复制、传播违法信息 | 符合[]  不符合[]  不涉及[ ] |  |  |
| 是否与用户签订注册协议 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 溯源管理 | 用户身份信息变更留存 | 是否对用户真实身份进行关联捆绑 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 日志留存管理 | 是否具有用户日志保存机制 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 信息联动管理 | | 是否具有联动信息的管控措施 | 符合[ ]  不符合[ ]  不涉及[] |  |  |
| 应急处置 | | 是否具备有效应急预案 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 是否设置7\*24小时应急电话 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 是否具有配套的安全应急处置技术手段 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 业务平台安全保障基线要求 | 业务平台部署 | 平台设置信息备案 | 是否具有详细的机房设备资产清单 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 设施境内外分布 | 是否具有有效限制境外违法信息在境内传播的管理措施和技术手段 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 资源调度 | 资源实时监控 | 是否具有对资源分配使用情况实施监控和日志记录的管理制度和技术手段 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 违法信息监测处置 | 是否建立有效违法信息处置的管理制度和技术手段 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 系统日志留存 | 是否建立有效日志留存的管理制度和技术手段 | 符合[]  不符合[ ]  不涉及[ ] |  |  |
| 用户接入要求 | 资质审核 | 是否具有严格的对接入用户身份的审核机制 | 符合[]  不符合[ ]  不涉及[] |  |  |
| 用户信息备案 | 是否对接入用户信息进行全面备案 | 符合[]  不符合[ ]  不涉及[] |  |  |
| 开放接口 | 是否具有严格的开放接口审核机制 | 符合[]  不符合[ ]  不涉及[ ] |  |  |

* + 1. 防范打击通讯信息诈骗安全保障能力评估

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **检查分类** | | | **检查指标** | | **检查结果** | **研判依据** | **证明材料** |
| **业务规范安全保障基线要求** | 业务规范管理 | 业务办理 | 申请主体资格管控 | 对于语音专线、“400”、“一号通”、“商务总机”、融合通信等电信业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 办理渠道管理 | 对于语音专线、“400”、“一号通”、“商务总机”、融合通信等电信业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 用户实名信息核验登记留存 | 对于个人移动通信业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 对于一卡多号类业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 对于语音专线、“400”、“一号通”、“商务总机”、融合通信等电信业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 防冒充行为管理 | 业务办理环节二次确认授权机制 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 自有业务端口类短信下发添加签名 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 业务申请数量管理 | 对于移动电话卡数量 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 对于“401”、“一号通”、“商务总机”等电信业务号码数量 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 业务落地号码管理 | 对于“400”、“一号通”、“商务总机”等电信业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 业务外呼管理 | 对用户申请“400”、“商务总机”外呼以及自带95、96等字头短号码通过租用语音专线 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 业务合同责任约束 | 对于语音专线、“400”、“一号通”、“商务总机”、融合通信等电信业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 业务认证 | 密码策略 | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 登录策略 | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 验证码策略 | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 业务认证数据安全 | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 业务登录提醒 | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 业务使用 | 台账管理 | 对于语音专线、“400”、“一号通”、“商务总机”、融合通信等电信业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 业务服务限制 | 对于涉及2个（含）以上基础电信企业省级公司的跨企业业务， | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 用户业务使用行为管控 | 对于一卡多号类业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 副号使用信息留存 | 对于一卡多号类业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 第三方管理 | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 用户个人信息保护 | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 业务核查 | 台账信息抽查复核 | 对于语音专线、“400”、“一号通”、“商务总机”、融合通信等电信业务， | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 业务使用复核监测 | 对于语音专线、“400”、“一号通”、“商务总机”、融合通信等电信业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 定期检查 | 对于语音专线、“400”、“一号通”、“商务总机”、融合通信等电信业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 企业内部考核问责 | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 异常行为用户监测管控 | 对于个人移动通信业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 跨企业业务号码核查处置 | 对于涉及2个（含）以上基础电信企业省级公司的跨企业业务 |  |  |  |
| 业务退出 | 业务注销 | 对于语音专线、“400”、“一号通”、“商务总机”、融合通信等电信业务 | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 技术管控 | 语音专线主叫鉴权 | 确保语音专线主叫鉴权比例达到100% | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 主叫呼叫过程的鉴权日志留存和稽核等机制及违规终止合作机制 | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 语音专线呼叫转移管控 | | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 外呼白名单管理 | | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 号码传送管理 | | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 通讯信息诈骗相关重点业务管理系统建设 | | | 符合【】 不符合【】 此项不涉及【】 |  |  |
| 针对网内和网间不良呼叫号码进行监测处置的技术管理系统 | | | 符合【】 不符合【】 此项不涉及【】 |  |  |

1. 安全评估结论意见
   1. 基础安全风险控制分析

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **风险名称** | **风险等级** | **详细描述** | **风险可控性研判** | **是否可控** |
| 网络存在被入侵的风险 |  |  |  |  |

* 1. 业务安全风险匹配性控制分析

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **风险描述** | **风险等级** | **详细描述** | **相应保障措施能力** | **风险可控性研判** |
| 信息载体难识别 |  |  |  |  |
| 信息内容难审核 |  |
| 信息传播跨平台对接，增大了识别监管难度 |  |  |

* 1. 安全评估结论

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **风险描述** | **详细描述** | **危害** | **整改建议** | **是否可控** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |
|  |  |

* 1. 同类业务的监管建议
  2. 业务部门初评总结签字确认表

|  |  |  |  |
| --- | --- | --- | --- |
| XX业务初评总结签字确认表 | | | |
| 业务名称 | XX业务 | 业务主管部门 | XX部门 |
| 业务介绍 |  | | |
| 初评结论 |  | | |
| 主管部门评估人员签字 |  | | |
| 业务主管部门领导签字 |  | | |

* 1. 信息安全管理部门复核总结签字确认表

|  |  |  |  |
| --- | --- | --- | --- |
| XX业务复核总结签字确认表 | | | |
| 业务名称 | XX业务 | 业务主管部门 | XX部门 |
| 业务介绍 |  | | |
| 复核结论 |  | | |
| 信息安全管理部门评估人员签字 |  | | |
| 信息安全管理部门领导签字 |  | | |

1. 附录
   1. 业务基础安全评估结果（详细）
      1. 资产清理
      2. 基线检测

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **问题类型** | **受影响设备** | **脆弱性名称** | **严重程度** |
|  |  |  |  |  |

* + 1. 漏洞扫描

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **类型** | **IP地址** | **操作系统** | **高危数量** | **中危数量** | **低危数量** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

漏洞列表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **问题类型** | **影响资产** | **漏洞名称** | **风险等级** | **备注** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

* + 1. 渗透测试
    2. 弱口令检查

未发现设备弱口令

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **IP地址** | **用户名** | **密码** | **应用程序** | **备注** |
|  |  |  |  |  |  |

* + 1. APP安全

本业务现阶段无App。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **受影响资产** | **漏洞名称** | **URL** | **严重程度** | **备注** |
| 1 |  |  |  |  |  |