数据平台安全设计报告

2016-10-27

1. **数据存储安全**

数据平台数据库部署在美国Amazon Web Services的云服务上，数据库本身不能通过在子网之外的环境访问，需要经过有安全验证的HTTP/HTTPS协议与应用服务进行通信，并且没有任何数据平台外的应用服务直接访问数据库。

1. **数据隐私安全**

数据存储在美国，不直接受到中国政府的监管，符合了美国、欧盟等对用户隐私数据保护协议的规定。和用户身份相关的数据在客户端得到用户授权许可之后才进行采集，由业务系统控制并承担责任。

1. **数据通信设计图**

/Users/Message/Downloads/-data_protocol.png

1. **数据通信安全详解**

**1、IP限制**，服务端-服务端的通信均有IP白名单或子网白名单进行限制

**2、签名**，客户端-服务端的通信使用APPKEY对内容进行签名，验证客户端的合法身份，避免产生脏数据。

**3、账号权限**，使用数据表同步和数据视图同步的服务，通过设置只读账号，且只能访问指定表或视图的方式来实现数据源数据的访问控制。

**4、HTTPS**，对于“单条即可产生价值”的关键数据，采用HTTPS的通信方式避免数据在通信过程中被第三方劫持的风险。

**5、权限隔离**，在可视化报表系统中，对各业务人员的访问权限进行隔离控制，由各业务负责人授权后才能得到数据报表查看权限。

1. **数据安全未来优化点**

1、数据平台早期发展时的人员授权比较混乱，如通过GT或EIM进行沟通，未经相关业务负责人进行邮件审批，接下来会导出各业务数据访问人员的清单，找业务负责人进行核查清理。

2、由于现阶段平台高速发展，缺少专门的运维来负责保障服务稳定运行，数据平台的开发人员持有部分数据查看的权限，在未来系统进入稳定期后，逐步收回开发人员的数据查看权限。

3、数据平台现在的APPKEY分发、人员授权以及和业务系统的对接处于半自动化的状态，存在一定的误操作风险和追责困难，未来要完善各种流程的自动化，增强系统性安全。

Message.miao 苗非繁

2016-10-27