**摘要:** 【问题】 在企业信息化推进的过程中，需要建设许多的信息系统，这些系统能够实现高效率、低成本的运行，为企业提升竞争力。但在设计和实现这些信息系统时，除了针对具体业务需求进行详细的分析，保证满足具体的业务需求之外，还要加强信息系统安全方面的考虑。因为如果一个系统的安全措施没有做好，那么系统功能越强大，系统出安全事故时的危害与损失也就越大。 请围绕“信息系统的安全性与保密性”论题，依次从以下三个方面进行论述： 1.概要叙述你参与分析设计的信息系统及你所担任的主要工作。 2.深入讨论作者参与建设的信息系统中，面临的安全及保密性问题，以及解决该问题采用的技术方案。 3.经过系统运行实践，客观的评价你的技术方案，并指出不足，以及解决方案。 【摘要】 2019年10月，本人所在保险公司启动了超级销售APP项目，该项目通过运用先进的销售工具、客户管理、营销活动管理等功能以达到提升销售人员的效能，加大业务驱动的目标。在该项目中我担任系统架构师，负责系统的架构设计工作。本文以该项目为例，主要论述了信息系统的安全性与保密性设计在系统中的具体应用。应用层方案，通过SSO鉴别登录，认证通过后基于角色访问控制加强用户权限管理；数据层方案，通过技术手段监控和记录网络内的服务器、数据库等设备的操作行为追踪审计，对于敏感数据加密后存储，保障数据保密性；网络层方案，将部署架构分为四个层次，互联网公网区、DMZ Web区、内网安全区、数据存储区，有效保障网络安全性。基于以上的技术应用，项目顺利上线，获得用户一致好评。

本人所在的保险公司分支机构遍布全国，已设立分公司36家，机构总数超过2100家，营业机构覆盖全国各个省份，系统员工人数超6万人。因保险生态体系的变革，各保险公司都在积极科技转型，公司基于新业态发展通过“线上化、数字化、智能化”加速推进“三新三聚焦”的战略转型。故启动了超级销售APP项目建设，本项目旨在建设业界领先的面向营销员的、具有前瞻性和可扩展性的，符合主流技术的保险销售一体化平台，聚焦核心作业功能，体现支持、服务、提效和赋能。系统主要实现功能车险、非车险出单、业绩管理、客户管理、营销活动、商业计划书、续保管理等。通过两个视角挖掘，营销员视角，集获客、展业、服务、个人成长为一体，作业辅导始终伴随的创新工作模式、挖掘潜在销售机会，提高工作效率，促进职业能力发展；管理视角，综合管理招募、培训、业绩、活动、提供营销指导和线索及客户服务锦囊，降低消息传递成本、提升营销员团队整体产能和绩效。  
该项目于2019年10月正式启动，我担任系统架构师角色，负责系统总体架构设计工作。在系统的实现过程中，系统的安全性及保密性是项目的基础，故在总体架构设计时对应用架构、部署架构进行多轮讨论并经过专家评委审核通过。下面基于此项目论述系统的安全性与保密性的具体应用。  
金融行业内的数据泄露打击是致命的，几乎每年也有相关案例的报道，所以要意识到安全性和保密性设计对整体架构设计工作的重要性。保障项目安全性不是从单方面几种安全措施能解决的，需要对项目全流程的梳理确认从硬件、软件、网络、应用、数据等方面检视。  
结合项目业务特点依次从应用、数据、网络三个方面着手针对系统身份鉴别、访问控制、数据完整性和数据保密性安全进行了充分的设计。下面将具体论述企业集成相关技术在本项目中的应用。  
1、应用层安全方案  
系统采用微服务架构模式，在应用层方面使用基于角色访问授权和接口服务加密等策略保证业务数据安全。客户信息、业绩管理等信息非常敏感，如果盗用账户信息或在数据传输中泄露将带来不可预估的损失。针对以上问题，用户登录使用SSO鉴别登录用户是否合法，防止撞库增加验证码及多次登录密码错误账户锁死，用户登录后基于角色访问授权机制，建立多种角色组，根据用户岗位分配不同角色组，满足业务需求前提下增强系统安全性。接口服务原因导致数据的泄露，企业中因业务的复杂性往往有很多异构的系统在运行，某些场景下需要集成多个应用服务完成一个任务场景，例如保单全单退保使用资金系统退费时，如何保证资金系统接口服务不被篡改保证数据的安全。基于此采用企业总线方式服务管理注册和注销，所有服务提供方及服务消费方需要申请授权在ESB登记后才可以进行访问，通过ESB可以屏蔽服务提供者相关信息，记录监控所有服务运行轨迹。同时服务接口数据使用加密处理机制，降低报文泄露后等风险。通过用户使用的角色授权，接口服务注册管理监控记录能有效提高系统安全性和保密性。  
2、数据层安全方案  
信息系统的数据库是企业的核心，其中涉及大量企业运营的数据，需保障数据的绝对安全。来自非法的数据访问和使用控制，数据脚本未经审核等程序操作造成业务数据丢失、篡改，未采取安全的方式处理敏感信息的输入和输出，信息被盗、篡改、故意或无意泄露。数据管理方面对数据采集、传输、交换、存储、备份、恢复和销毁等环节出现未经批准导致数据泄露，存储介质不可用导致的数据损坏。针对以上存在数据安全方面的问题，主要通过数据访问和使用控制，数据管理两位维度进行规划。通过堡垒机敏感操作平台控制用户角色权限，控制用户对服务器、数据库、目录、文件等网络资源的访问。执行的数据脚本提交DBA审核，操作流程采用层级式管理，重要数据操作采用层级审批，运维实时监控。数据库服务器主从库机制备份，系统遭遇故障和灾害时能迅速切换到正常服务器，保证信息系统能正常运行，数据信息每天全备和实时增量备份，当数据信息造成意外丢失和损坏时，可快速切换恢复数据。  
3、网络层安全方案  
超级销售APP是面向互联网的应用，因为网络和硬件是整个系统运行的基础，在面向公网的应用很容易遭到网络攻击，拒绝服务攻击、木马植入等多种手段造成应用服务的不可用。针对上述情况我们将整个部署架构设计分为四个层次，互联网公网区、DMZ Web区、内网安全区、数据存储区。互联网公网区为超级销售APP运行访问，支持手机APP、微信公众号体系在互联网公网访问。DMZ Web区为内网非安全区域，进入此区域所有的请求会经过防火墙和Nginx反向代理中转。内网区为内网安全区域，外部用户和系统是不能直接访问，处于网络隔离环境中，DMZ Web区的网关通过开通网络策略点对点开通访问权限，此区域主要部署应用微服务和内部管理服务器，后台管理和监控管理服务器。数据存储区，数据存储区域为内部核心区域，物理上可以和内网安全区在一个区使用网络策略，隔离是安全级别最高的区域，主要部署数据库Mysql、分布式缓存Redis等服务器。通过上述网络部署规划极大提高应用服务、数据库的安全性。  
整个项目历时9个月的实施，于2020年7月完成验收并顺利上线，日均出单保费规模达到千万级别，赢得了良好的用户口碑也在业界内树立了标杆。  
通过应用层、数据层、网络层三方面安全的设计规划，提高了系统的安全性、保密性达到项目预期的效果。为了充分检测验证系统的安全等级，通过对系统全面安全检测从客户端数据、静态安全、运行时安全、安全策略设置、网络通信安全、业务安全多维度扫描，发现网络通信端与服务端缺少证书校验，存在通过伪造证书等手法进行攻击获取信息。针对这种情况客户端校验服务器端证书的有效性，可通过公钥绑定的方式进行校验，防止伪造证书手法获取信息。基于信息系统的安全性与保密性设计思想，能有效解决企业信息泄露风险。接下来还会继续不断完善系统安全方面的设计缺陷和不足，保障系统安全稳定运行。