XX 单位/XX 公司 XX 系统
平安方案设计

编制日期：2018 年 5 月

书目

1 背景

随着全球信息化的发展，互联网应用渗透到了各行各业。互联网金融借助互联网技术、移动通信技术，实现金融资源优化配置和应用普及，互联网金融的出现代表一个新兴金融时代的到来。随着第三方支付、移动支付、P2P 信贷、众筹融资等互联网金融概念已经被各方炒作的如火如荼、方兴未艾。在 2014“两会”上，“互联网金融”首次出现在国务院总理李克强所做的《政府工作报告》中。激励互联网金融创新、为“余额宝”正名、加强互联网金融监管成为“两会”代表的共识。而传统金融行业在市场的倒推下也面临着经营理念、经营方式、业务体系、战略渠道上的全面转型。

信息流、资金流的平安性是互联网金融发展的基础和保障，随着棱镜门、钓鱼网站、网银盗窃等互联网平安事务层出不穷，不法分子犯罪技术不断提高，犯罪手段花样翻新。而一旦遭遇黑客攻击，互联网金融的正常运作将会受到影响，危及消费者的资金平安和个人信息平安。2014 年的“两会”中，互联网金融的平安性成为备受关注的焦点，除了法律法规、相关制度和行业标准不断完善的顶层设计，通过技术手段爱护数据平安，防范黑客攻击已成为保障互联网金融平安的必要举措。

2 系统现状分析

2.1 互联网金融行业平安现状

- 攻击: 数据显示，金融行业被 DDoS 攻击次数仅次于嬉戏，直播等行业；

  2016 下半年，国内 500 强金融机构遭到 600 次 DDoS 攻击，近三成为 CC 攻击。

  互联网金融行业遭到攻击的状况尤其严峻
- APP 仿冒：89%的热门应用被仿冒；55%仿冒应用具有恶意行为；某金融机构发觉 30 多个仿冒应用，全部出现劫持用户短信的行为
- 信息泄露：金融机构对信息泄露的敏感度远大于其他行业；信息泄露不但给自己造成巨大的损失；也为对手送去了极佳的机会；
- 漏洞：报告显示，互联网金融行业的漏洞存量在金融行业名列前茅；大量漏洞未经处理，被利用的难度极低

2.2 系统信息平安现状

目前我公司信息系统部署在阿里云，购买 ecs 服务器、负载均衡 SLB、数据库 RDS、数据库 Redis，OSS 文件存储。

运用 vpn 进行 ECS 服务器的管理，运用阿里云盾中安骑士基础版，仅有检测漏洞的功能，（对标 cve 官方漏洞库，自动检测并供应修复方案）