## ****内容介绍****

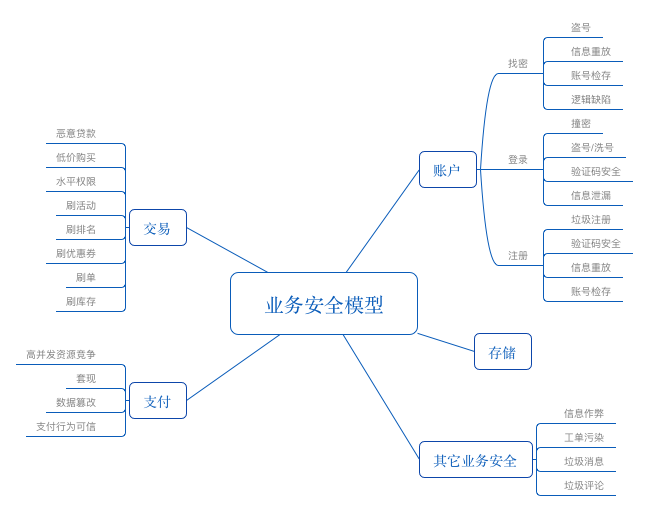
本篇是系列文章的第十篇，分享一下自己对业务安全的理解。

## ****业务安全是什么****

业务安全的目的在于，让业务正常开展，持续提供**预期**的服务。业务安全工作，是**围绕着业务**构建一系列安全风控的制度、工作流、系统、工具、风控规则、运营体系。

业务安全不像应用安全/基础IT设施安全等安全方面具备普适性，它需要紧密围绕业务来构建。

业务不同，业务安全的措施也不同。



上图是我在互联网找到的一个业务安全模型。

其中的密码找回，权限问题，跳步骤问题等等，这些我不认为是业务安全的问题，它的业务设计、功能设计等都是正常的，有问题的是应用安全问题，是代码实现有漏洞。

其中，业务安全问题应该是薅羊毛问题、爬虫问题、黑灰产问题、坏账问题、水军问题、刷单问题等。

代码实现的问题，责任在程序员。业务设计问题，责任不在程序员。

## ****业务安全需求来源与演变****

所有企业本身就有业务安全的需求。业务安全并不是一个新的事务。业务安全只是一个新的词。

互联网之前，大部分行业都已经存在，其业务安全问题，在长时间的发展历程中，就已经得到了解决，比如风控。

但是随着互联网的发展，以及互联网对行业的业务形态的改变，传统的风控措施失效了，而且业务面临了新的，从未有过的业务安全问题。比如电商平台的刷单，在电商平台之前，刷单不会成为业务安全问题，刷单这个行为也不会出现。因为电商平台的出现，商家为了打造爆款，取得消费者信任，出现了刷单这个行为，而这个行为，破坏了电商平台的业务。消费者借鉴电商平台给出的销量数据，但是从平台的商家买到的是名不符实的产品。这样，电商平台受到的损害更大。商家收到钱了，不行商家可以在别的平台开一家新店，但是电商平台没法改头换面。

传统风控失效的同时，恰逢网络安全行业的发展，网络安全里顺势提出了业务安全这个词。

而且网络安全，更懂互联网，也更懂技术，可以很好的解决这些从互联网而来的业务安全问题。

## ****业务安全理念演变****

没有通用的业务安全，也就没有通用的业务安全理念。

可能在具体行业里，有发展的比较成熟的具体行业的业务安全理念。笔者对这些不是很了解。

这里借原神与魔兽，聊一下游戏行业的业务安全问题。

1. 私服

魔兽世界因源代码泄露，导致魔兽私服的产生。其根源是数据信息安全方面的问题。但是魔兽私服，直接导致玩家流失，直接造成业务安全问题，修复数据安全问题无法解决这个业务安全问题。

原神私服，其本质并不是一个私服，只是一个抽卡模拟器。它没有后端的服务，无法实现正常原神的游戏功能。黑灰产人员，他卖的只是自己破解魔改之后的原神客户端而已，是一种对玩家的欺诈。

私服问题，游戏公司的通用措施都是诉诸法律。可能会假装玩家去提醒玩家私服的资金安全性，游戏合法性，游戏体验性等问题。为什么说可能呢，因为提醒本身也是一种引流，可能导致未接触到这个信息的玩家，反而通过官方引流，去到了私服里去。

1. 机器人签到奖励问题

每个版本，原神都有微博签到奖励原石的活动。而且，米游社里，也有每日签到跟原石兑换的活动。

原石是抽卡资源。抽卡充值直接影响米哈游的营收。

但是初期其这两项活动，都没有做人机验证。所以导致有一次，微博的签到奖励发完了。正常玩家最后一天签到完成之后，普遍在微博反映，原石发完了，怎么回事，以前从没有发完过。其实就是被机器人刷了。

米游社的原石兑换也是如此，正常玩家在19：00都抢不到，秒没。

这些工作室在获得兑换码之后，会放到淘宝去卖。

1. 社区水军抹黑

任何游戏，任何公司，都可能遭遇水军抹黑。遭遇舆情事件，品牌形象受损。

这种情况，如果发生在自己控制的社区中。是有可能，通过揭露水军身份，证明抹黑行为，反而实现舆论的翻身仗的。

通过注册社区的信息，可以关联到其游戏中的信息。比如其游玩时间，熟练度，等级，战力，充值金额，年龄，IP，同身份账户，游戏异常行为等等。

将这些信息，汇总整合，正面回应抹黑舆论，并指出其抹黑行为，能够打一个翻身仗。

社区设计，也可以设计成，社区用户的一些非敏感信息，能被其他用户通过主页看到，辅助用户对其身份及言论进行相关判断。

1. 外挂作弊

不论是单机游戏还是MMO游戏，都会遇到外挂作弊问题，而且这个问题会永恒存在。

因为客户端是在用户本地电脑上的，可能被破解的。技术是在攻防之间不断进化的。

原神的游戏模式，是单机模式。外挂对其他玩家，跟自己业务模式的影响很小。所以它对外挂的处理措施就比较轻，通常都是封号了事。

但是MMO外挂的破坏性就非常大，游戏公司通常会联合警方直接捣毁外挂团伙。

技术上，要不断提高作弊难度，比如加壳，比如绑定反作弊引擎。还可以根据具体情况实现不同的反作弊手段。而且这些手段一定要是服务端判断的。比如梦幻西游的人机验证，比如CS的战绩作废等等。

1. 账号买卖

正常的账号买卖不对业务造成影响。而且游戏公司也管不到这个，也没有法律管这个。

但是异常的账号买卖就对业务造成影响。异常账号一般是通过机器人练的资源，或内鬼生成的账号。

机器人问题跟前面的反作弊一样，内鬼问题则是办公安全方面的问题。

1. 工作室问题

工作室是机器人的升级版。但是其危害比机器人其实大出了一个量级。因为机器人只造成零散的影响，但是工作室一定对整个游戏生态都造成非常大的影响。最明显的就是，机器人可以封账号，但是面对工作室，封帐号一点用都没有，需要构建更体系化的业务安全措施。

## ****业务安全的建设落地****

步骤：

应急跟需求：处理应急跟公司需求

状态调研及评估：调研安全建设状态，评估建设完成度。

决策工作内容：结合调研结果，结合公司整体的建设方案，来决定工作内容，内容顺序，落地方案。

根据优先级，去对具体业务做针对性的理解。理解其业务流程，功能设计，预期结果，再结合自身对互联网及黑灰产的认知，具体分析其业务安全是否存在问题。

业务安全方面的建设，要紧密围绕着业务进行。然后分析出来的具体问题及实现措施，可能落到其他安全方面，也可能落到非安全领域。

业务安全非常考验人的思路及知识面。

## ****业务安全与其他安全方面的耦合****

应用安全等方面出现问题，都会对业务造成影响。业务出现问题了，其根源可能不是业务安全问题。存在业务安全问题，其他安全方面都很好，业务一定会出现问题。

## ****总结****

业务安全是新的词，不是新的需求

业务安全问题的根源，在业务设计产品设计

业务安全没有通用方法论，是紧密围绕业务的

互联网时代的业务安全，可借鉴传统风控做互联网优化

业务安全非常考验思路跟知识广度

## ****QA****

弟弟失业中，目前在上海，正在找工作。各位大佬如果对我感兴趣的话欢迎加我VX：qinbingjie1101