账户体系安全管理探讨——安全小课堂第十一期

京东安全应急响应中心 2016-05-20

安全小课堂第十一期

账户体系控制不严可通过授权控制访问不属于自己的数据，泄露敏感信息，导致不可直视的后果。

本期我们邀请到网易安全专家沈明星、唯品会安全专家悟空，来和我们来探讨下账户体系的安全管理~

1

豌豆妹

账号体系管理包含哪几部分呢？

葫芦娃

分为登录、注册、找回密码、消除、冻结。

1.其中登录、注册得区分正常、撞库、暴力破解、秒杀及羊毛党用户；

2.找回密码涉及业务方对安全的认知度还有安全的规范与否，这个占很大比重。如果产品和开发对安全认知深浅不一，那就会面临各种各样的安全隐患；

3.消除和冻结，比如在电商行业里一个被风控行为指定为专门用来做秒杀的用户那就会触发冻结规则，而所说的消除得看行业和业务（目前应该很少有这种规则）。

2

豌豆妹

聊聊账号体系面对的一些内外部风险呗~

哆啦A梦 

从外部风险先说起。在注册阶段，会有针对注册机、垃圾虫注册垃圾账号，以便于后面养账号、买卖账号，进一步的通过垃圾账号秒杀，抢红包，发垃圾等等。在登陆阶段，遇到最多的就是暴力破解和撞库攻击。我们需要的还是立体的、多层次的防御体系。另外，在密码找回阶段，主要由于一些历史原因或者设计的不合理，往往也会成为攻击者喜欢下手的地方。最后就是公司对账号的主动回收，这个因账号体系而异。还有就是当前账号是正常、被盗、申诉等状态的，需要细化的策略去分析出来。

豌豆妹

那我能理解成：用户的行为导致被回收吗？

小新 

长期不登录不活跃的用户账号，会有回收机制。这个得看业务。当然这个也会造成一些安全上的风险。

小丸子 

主要还是这块儿设计上比较复杂，各类密保一环套一环，然后有时候一改动或者增加

一个新接口，就容易出事儿。这个可能是邮箱账号特有的问题。比如，A君拿邮箱注册第三方服务，如果A君长期不登录邮箱，导致邮箱被回收,那么A君注册第三方服务，可能被人重新注册邮箱后，通过邮箱找回密码的方式，盗取第三方服务的账号。

豌豆妹

那这块的回收机制是不是还有另外的一些策略，比如此账号长期用来秒杀特定活动，垃圾信息推广等？

葫芦娃 

这个要看具体的风控策略是如何划分了，有时候得分业务去考虑情况。

3

豌豆妹

账号体系风控成熟的架构是哪种形式呢？

哆啦A梦 

大致都是在线的风控+离线风控结合，然后规则 vs 模型。一般得二者配合起来。数据支撑第一位，埋点信息足够多，能完整跟踪用户的整个行为。

小新 

在线的一般是需要实时返回，主要采集位置、时间、网络环境、行为等数据。

豌豆妹

那会分档位吗？比如1-10，异地登录情况算2，不在常规设备算3。比如6分以下直接过，7分弹验证码，8分验手机，10分直接阻断。

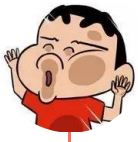
哆啦A梦

嗯嗯，一般最后算一个分出来。验证码也可以分不同等级，等级越高粘连度越高。但是黑产也会识别验证码，神马打码平台，人工打码等等，所以风控策略需要经常评估有效性。我们能做的就是不断提高攻击门槛，或者让攻击者无利可图，且不太影响用户体验。

4

豌豆妹

如何划分风控策略的维度呢？



小新

可以从以下几个来划分。

1.账号：经过风控策略分析确认该账号的类型是正常、被盗、申诉状态等等；
2.设备：一个账号最多能登录几台设备，同一账号下每台设备的切换是否需要证明用户身份，同一个设备频繁切换不同，用户会触发什么等级的阈值规则;
3.位置：也就是非同一地区登录的验证规则，如果同一地区触发较多的异地状态是否也会触发规则；
4.行为：举个栗子🐱。用户三次访问JD，第一次访问之后直接查看我的订单，因为昨天刚买了一台Mac电脑看看现在到哪了。第二次访问这台电脑的商品页，然后退出。到了第三次访问之后直接下了一单Mac，发现需要支付密码然后找回支付密码，发现找回又需要提供身份验证....第三次异常的行为记录又是会触发什么样的规则，还有具体的策略要如何去细化；
5.偏好：其实这块可以涵盖到用户行为里面，不过可以把每个用户的操作习惯记录下来，有非常态的操作触发风控规则；
6.关系：也就是朋友/设备/买家与商家各种关系的状态，比如一个存在泄露买家信息的商家，与他交易甚多的买家是否会触发规则。

5

豌豆妹

大家聊的很给力呢，那咱们理想的内部风控流程是什么样的呢？

小丸子

概况来说，一个门进来，分很多条路，最后让坏人的路越走越窄。

葫芦娃

前阵子接手的一国外内部同事开通内部账号的问题，当时想着在流程上所有的增删改操作都能跟总部关联起来，预防一些他们自己运营引起的安全风险，确定人员运营系统权限的地步。

比如从技术架构上，确定内部人员的操作权限到底能到什么地步，如何不依赖于人而是依赖于严格的授权机制。敏感业务的授权理论上应该做到即使是内部工作人员也不可能利用工作之便获取用户权限。从业务流程上对某种情况的处理设计的是否合理没有漏洞可钻，这样内部流程才会逐步完善。

安全小课堂往期回顾：

1、论安全响应中心的初衷；
2、安全应急响应中心之威胁情报探索；
3、论安全漏洞响应机制扩展；
4、企业级未授权访问漏洞防御实践；
5、浅谈企业SQL注入漏洞的危害与防御；
6、信息泄露之配置不当；
7、XSS之攻击与防御；
8、电商和O2O行业诈骗那些事儿（上）；
9、电商和O2O行业诈骗那些事儿（下）；
10、CSRF的攻击与防御。

JSRC http://security.jd.com/

长按识别左侧二维码，关注我们