CNUTCon 2017
全球运维技术大会

麻袋理财安全与合规建设

王耀

麻袋理财 中信产业基金控股

主办方 Geekbang 极客邦科技 InfoQ

Geekbang.
极客邦科技

极客搜索

全站干货，一键触达，只为技术

s.geekbang.org

扫描二维码立即体验

有没有一种搜索方式，能整合 InfoQ 中文站、极客邦科技旗下12大微信公众号矩阵的全部资源?
极客搜索，这款针对极客邦科技全站内容资源的轻量级搜索引擎，做到了!

扫描上方二维码，极客搜索!

EGO EXTRA GEEKS' ORGANIZATION NETWORKS

这里只有
技术领导者

EGO会员第二季招募季正式开启

报名时间：9月1日-9月15日

扫描添加E小欧，

邀您进入EGO会员预报名群

立即报名

E小欧

先来讲一下这个分享的主题

今天的分享计划

不谈具体的某项技术， 听众群体不是面向白帽

今天的分享目的

甲方安全核心的方向， 大部分企业都可以落地的

关于我

王耀　麻袋理财信息安全负责人

擅长　企业信息安全治理

CEH　CISSP

TABLE OF **CONTENTS**

麻袋安全团队介绍

我们的发展历程

2015年11月 → 安全诞生 → 一个人的安全部 → 眉毛胡子一把抓

2016年7月 → 新同事加入 → 应急响应 → 渗透测试、安全策略、合规

2017年5月 → 安全团队正式成立 → 业务安全 → 安全工具 → DLP

安全必须独立于开发/运维的必要性

1.专业技能不同，攻防视角不同

2. 各类安全问题不断增加，需要高效的处理

3. 法律法规合规性要求

4. 需要“背锅侠”

麻袋理财安全团队职责

防范黑客

控制风险

合规建设

SMD-Team 团队构成

Web/APP 渗透狮

内网 渗透狮

应急响应与反制

取证/合规专员

岗位要求：

- 一专多能
- 岗位联动，A-B角
- 24h Standby

渗透测试

安全扫描

自研工具

安全制度

DLP

安全审计

安全意识

应急响应

安全团队的日常工作

TABLE OF **CONTENTS**

我们怎么做安全

信息安全框架

数据安全

数据丢了是雷区

业务安全

业务系统被黑客入侵了麻烦大了

安全合规

安全合规岂能不重视

数据安全

STOP THIEVES

防**黑客**盗数据，防**“内鬼”**

数据安全-数据安全生命周期

遇到的
痛点：

数据导入很简单？
保存又不是问题？
使用那还不简单？
传输管我屁事？
用完就随便扔？
偷数据找不到人？

仅限于这些吗

核心的
方法：

合理**脱敏**
强制**加密**
分层审批
最小特权
数据库审计、防火墙、数字水印
……XXX

仅仅是冰山一角

业务安全

信息安全

日常工作

- 互联网泄漏信息扫描
- web/app/内网渗透测试
- 应用上线/版本迭代更新安全检测
- 漏洞安全预警/建立知识库
- 安全应急响应/天眼漏洞扫描系统/IPS/数据库审计

攻防安全

麻袋安全应急响应中心（MDSRC）

- 公众渠道建设
- 平台漏洞收集
- 漏洞成因分析
- 应急响应定期演练
- 安全编码/攻防技术研究

应用安全

- WEB安全
- APP安全
- 内网主机安全
- 第三方外包产品安全
- 软件开发安全

架构安全

- 内网监控
- 网络安全
- 系统安全
- 等保、ISO27001建设

安全防护

- NIPS
- HIPS
- WAF
- 安全运维中心（SOC）

- 蜜罐、github、网盘爬虫、自研安全工具

安全管理

- 安全制度、规范
- 安全流程
- 安全检查
- 安全内控
- 安全审计
- 安全月报
- 安全培训

遇到的
痛点：

业务流程**复杂**？
没有安全技术**大牛**？
落地难，跨部门不配合？
管理层**不认可**？
三分技术，**七分**管理？
缺钱，缺人？

仅限于这些吗

推荐的
方案：

深入**熟悉**业务
适度**外包**
业务**优先,**做好**沟通**
Actions **S**peak **L**ouder
谁三谁七，也**不一定**
招人，加大预算 **or 小米+步枪**

仅仅是冰山一角


然后，我
们来讲下
合规

安全合规

1. 《互联网金融网络与信息安全技术指引（试行）》
2. GB/T28448-2012《信息安全技术 信息系统安全等级保护测评要求》
3. 《网络安全法》

互联网金融行业的合规，对于数据安全的要求尤为突出

2016年12月通过三级等保测评

项目编号：SHTEC2016DSYS508

等级测评结论

测评结论与综合得分			
系统名称	麻袋理财核心业务系统	保护等级	第三级
系统简介	上海凯岸信息科技有限公司建立了一套具有较强的业务处理能力的麻袋理财核心业务系统，承担了该系统的运行维护业务，信息技术部对该系统具有信息安全保护责任。 该信息系统业务主要包含：前端和后端；前端对外针对公众提供互联网金融产品交易服务，主要包含麻袋理财官网 www.madailicai.com、麻袋理财移动端 APP 及网站应用管理后台，其中，官网和移动端 APP 提供 2dit 处理联机交易的功能，"我的账户"计算用户的产品购买记录和产品收益，以及用户的账户信息，主要包括：用户充值、用户提现、产品购买及转回功能。后端，主要是提供给员工进行相关的业务操作，并配有相应的权限管理。		
测评过程简介	受上海凯岸信息科技有限公司委托，上海市信息安全测评认证中心于 2016 年 9 月 8 日至 2016 年 12 月 23 日对麻袋理财核心业务系统进行了系统安全等级测评工作，本次安全测评的范围主要包括麻袋理财核心业务系统的物理环境、主机、网络、业务应用系统、安全管理制度和人员等等，安全测评通过静态评估、现场测试、综合评估等相关环节和阶段，从主机安全、应用安全、数据安全与备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理八个方面，对麻袋理财核心业务系统进行综合测评。		
测评结论	基本符合	综合得分	89.53 分

等级测评结论 -IE-

遇到的痛点：

合规要求**数量多**？

现有的系统**很复杂**？

成本、预算、效果的平衡点？

仅限于这些吗

麻袋的方案：

内外部**风险识别**

管理层支持

安全**技术**控制

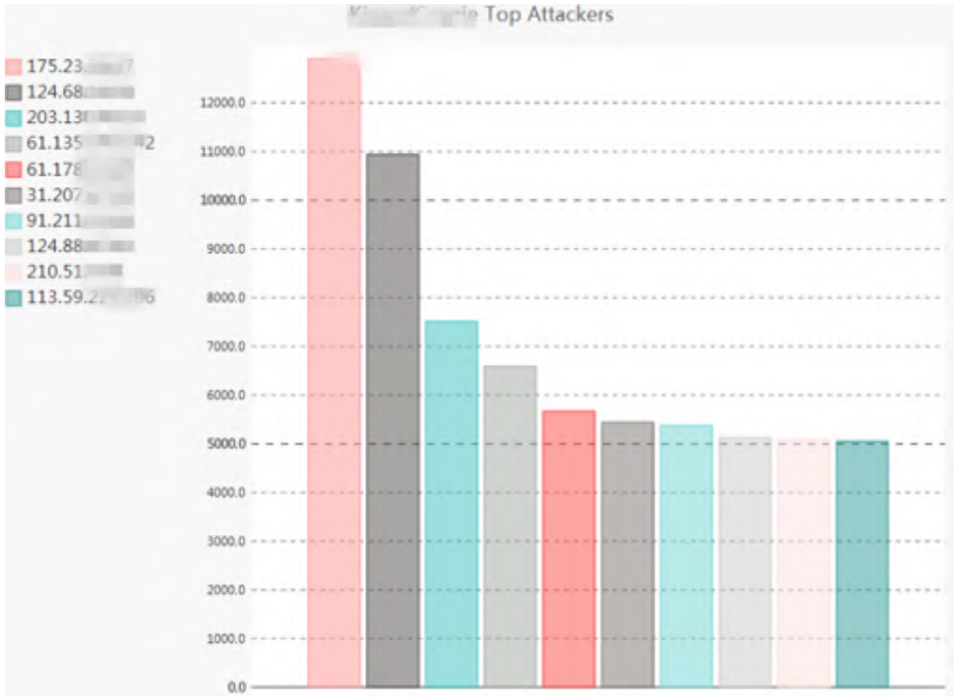
管理策略落地

跨部门协作

总体的思路

一周 Web 攻击统计图

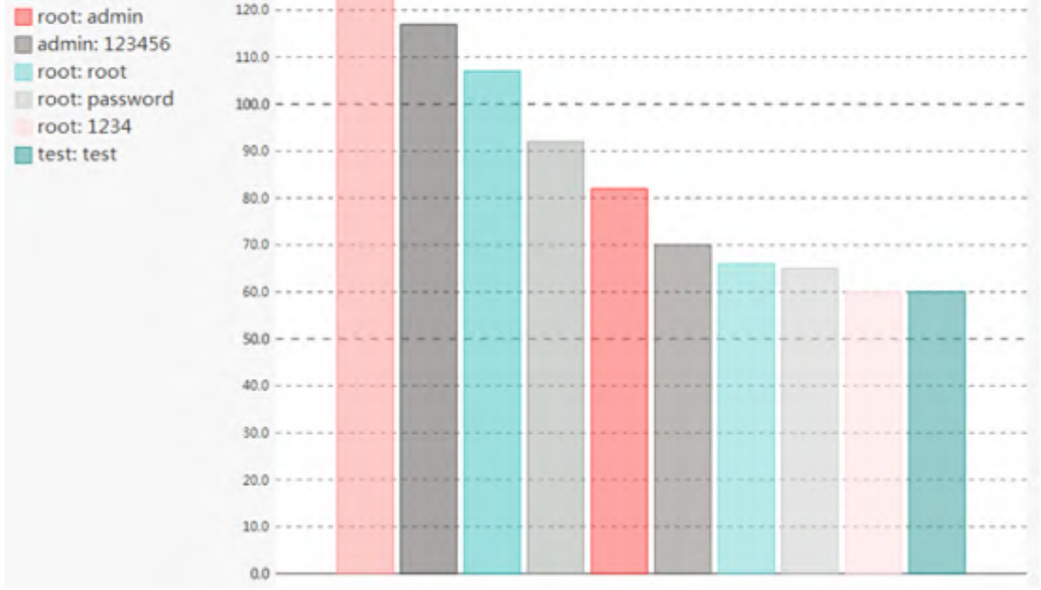
IP	所在地址	COUNT
123.59.1	北京市大兴区天地祥云 BGP 数据中心	8
123.59.13	北京市大兴区天地祥云 BGP 数据中心	
54.175.12	美国华盛顿州西雅图市亚马逊(Amazon)公司数据中心	
91.223.13	乌克兰	
163.172.12	英国 CZ88.NET	
138.197.13	美国纽约市 DigitalOcean 云公司	
104.131.0	美国纽约市 DigitalOcean 云公司	
195.154.6	法国 ONLINE S.A.S.数据中心	
71.74.184	美国弗吉尼亚州费尔法克斯县赫恩登镇时代华纳有线互联网有限公司	
85.113.20	俄罗斯	
60.175.18	安徽省滁州市电信	
84.72.17	瑞士 CZ88.NET	



本周发现来自 ip 123.59 的攻击访问。通过日志分析，攻击来源 ip 在 7 月 28 日 17:19-17:44 频繁访问蜜罐的 b 应用，发送了近 29815 条攻击数据，蜜罐完整记录了攻击使用的 payload：

2017-07-28 17:44:56	ubuntu		123	80	http
2017-07-28 17:44:56	ubuntu		123.59	80	http
2017-07-28 17:44:56	ubuntu		123.59	80	http
2017-07-28 17:44:56	ubuntu		123.59	80	http

```
2017-07-28 17:19:03,513 ( ) 123.59.  6 requested GET /?nx=88 on ubuntu:80
2017-07-28 17:19:03,603 ( ) 123.59.  6 requested GET /Admin_Files/ on ubuntu:80
2017-07-28 17:19:03,739 ( ) 123.59.  6 requested GET / on ubuntu:80
2017-07-28 17:19:27,586 ( ) 123.59.  6 requested GET / on ubuntu:80
2017-07-28 17:19:28,205 ( ) 123.59.  6 requested GET /robots.txt on ubuntu:80
2017-07-28 17:19:28,829 ( ) 123.59.  6 requested GET /pagina.php?index on ubuntu:80
2017-07-28 17:19:28,892 ( ) 123.59.  6 requested GET / on ubuntu:80
2017-07-28 17:19:28,913 ( ) 123.59.  6 requested GET /pm/add_ons/mail_this_entry/mail_authocher
2017-07-28 17:19:28,942 ( ) 123.59.1  requested GET /side/jee/ on ubuntu:80
2017-07-28 17:19:29,021 ( ) 123.59.1  requested GET /includes/ on ubuntu:80
2017-07-28 17:19:29,026 ( ) 123.59.1  6 requested GET /index.php?base_dir on ubuntu:80
2017-07-28 17:19:29,036 ( ) 123.59.1  6 requested GET /side/jee/general.php?abre on ubuntu:80
2017-07-28 17:19:29,068 ( ) 123.59.  6 requested GET /pm/add_ons/mail_this_entry/ on ubuntu:80
2017-07-28 17:44:27,259 ( ) 123.59.1  requested GET /includes/includes/config.php on ubuntu:80
2017-07-28 17:44:27,268 ( ) 123.59.1  requested GET /index1.php on ubuntu:80
2017-07-28 17:44:27,277 ( ) 123.59.1  requested GET /cgi-bin/new-visitor.inc.php on ubuntu:80
2017-07-28 17:44:27,286 (glastopf.g 123.59.1  requested GET /index1.php on ubuntu:80
```



自研工具-蜜罐：捕捉黑客的攻击IP/行为分析/爆破口令

传统商业漏洞扫描器的痛点：

1、扫描周期长、扫描库更新不及时；

2、漏扫系统每次加载扫描器中所有规则，导致报告中信息堆砌，产生诸多干扰项；

3、漏洞情报信息获取不及时，无法第一时间，响应错失修补漏洞最佳时机；

4、漏洞预警只报告受影响的系统版本及范围，具体公司哪些资产受漏洞影响，需要运　维和安全人员进行排查，应急响应过程相当繁琐；

“天眼”系统的优势

1、能对公司拥有的所有资产进行识别统计

2、每次有突发漏洞通告时，天眼系统将自动关联资产进行自动化漏洞验证

3、大量节省漏洞预警时间和人力发现过程。

自研工具-“天眼”漏洞预警系统：实现漏洞自动告警

TABLE OF **CONTENTS**

思考

面对日趋复杂的网络环境，如何应付“杀链”

1、如何防范APT攻击？（水坑、鱼叉式攻击等）

2、对攻击者如何做到追本溯源？（蜜罐、攻击历史画像、借助外部团队力量）

THANKS!

智 能 时 代 的 新 运 维

CNUTCon 2017