安全小课堂第六十八期【安全运维的那些事】

京东安全应急响应中心 2017-08-04

运维安全是企业安全保障的基础，与web安全、移动安全、业务安全等环节共同构成了企业的安全防御体系。并且运维出现安全问题危害严重。因此，因此运维安全往往是企业开始做安全的第一步。JSRC **安全小课堂第六十八期**，邀请三位老师分享安全运维的那些事，本期小课堂邀请到了HRay、**Rozero**、**LS**老师进行分享。同时感谢JSRC白帽子们的精彩讨论。

安全运维的主要工作有哪些?

京安小妹

首先日志是一个系统中很重要的一部分,正常情况下可以通过日志进行错误排查，作为性能优化的参考等。
在安全方面，可以发现一些异常的行为，比如频繁的登录失败、不正常的URL请求等等;
很多的蛛丝马迹都可以从日志里边看出来。

讲师： HRay、Rozero、LS

日志审计能主要审计内容（网络安全方面）有哪些?

1）主动发现运维相关安全问题并想好应对措施。
2）查看IDS、IPS、WAF、主机IDS等常见安全设备报警并处理。
3）安全事件的应急响应。
4）完善各类安全监控。
随着公司环境不同工作内容也会有些变化，比如小公司可能分工没有那么明确，要求发现问题，找出解决方案到方案落地及后期维护都由一人解决，大公司往往分工比较明确，一般都有专人负责事件推动

甲方安全工作涵盖较为繁杂，需要保障办公、生产及线上生产环境安全稳定运行。以甲方为例：
1、工作可能包含堡垒机、防火墙等安全设备的维护及安全策略更新。
2、负责网络的安全域划分隔离。负责新上线业务的主机、业务加固与加固基线定制。
3、负责上线前的主机安全检查及漏洞扫描。负责上线后的业务安全持续监控，及做必要的日志分等工作。
4、同时也会做一些入侵检测规则及日常安全事件的处理及响应。

监控巡检：对网络架构、网络设备、安全设备、服务器主机、操作系统、数据库和用户账号、口令等进行监控与定期巡检，了解信息系统的运行情况，同时进行周期性安全评估。
审计：对各类安全系统、应用类系统日志进行审计与分析，检查策略是否有效，配置是否安全，是否有可疑事件发生，包括防火墙、入侵检测/入侵防护、DDOS防护系统等等。
安全加固：基于日常监控、渗透测试、风险评估中发现的安全风险，制定相应的安全策略，加强信息系统的安全性。
安全意识培训：加强运维人员个人的安全意识培训。
安全建设：根据业务发展，完善信息安全体系建议与规划。
安全事件处置与应急预案：针对各类系统的安全情况，制定对应的应急预案，当出现重大安全风险时，以保障业务的安全稳定运行。
关注行业安全情报，了解实时的安全漏洞、厂商安全通告，及时对安全漏洞进行修复。

安全运维主要能避免什么样的安全问题?

京安小妹

一般各种系统或程序的弱口令，服务配置不当导致的各类问题，端口对外乱开放以及主机被入侵后的及时发现等都需要安全运维解决。

安全工作的建设主要目的在于防患于未然。
安全工作的有效进行，能够使得业务在上线前、中、后多个维度受到保护。以漏洞为例，某个漏洞事件爆发前，我们就已经通过渠道获取到了情报，并且明确事件的影响范围及可能受到影响的系统及版本。及时联系开发/运维将漏洞修复。并且在系统中加了相关的监控规则，当漏洞大规模爆发时，我们就可以不受到任何威胁。

人为的安全问题：弱口令、配置不当、权限滥用等。
系统安全问题：安全漏洞、程序BUG等。

讲师： HRay、Rozero、LS

安全运维工作需要具备的能力有哪些?

京安小妹

精通网络安全技术：包括端口、服务漏洞扫描，程序漏洞扫描分析检测、权限管理、入侵和攻击分析追踪、网站渗透、病毒木马防范等；
熟悉TCP/IP协议，熟悉Sql注入原理和手工检测、熟悉内存缓冲区溢出原理和防范措施、熟悉信息存储和传输安全、熟悉c、数据包结构、熟悉DDOS攻击类和原理有一定的DDOS攻防经验；
各类安全漏洞的原理、漏洞扫描工具的使用、系统加固的流程和技术、入侵检测和追踪等；
具有网络脆弱性分析和渗透力测试的能力，能够熟练处理各种病毒和攻击事件，并且对其进行安全加固；
理解各种网络层及应用层拒绝服务攻击的原理，熟练使用抗DDOS技术和设备；跟踪并分析最新的安全漏洞，响应公司发生的应急安全事件；

1、从业安全工作需要具备扎实的攻防能力及计算机基础功底。
2、了解网络、系统的特性，能够对常见漏洞的原理及修复做到心中有数。
3、且需要具备丰富的运维能力，业界有句老话“一个经验丰富的黑客必然是一个出色的管理员”。
4、新时代的安全运维需要具备一定的数据分析能力，样本及日志数据越来越复杂，没有数据分析能力做起来会较为吃力。

1）了解常见的运维相关安全问题并知道解决方案。
2）可以看得懂IDS、IPS、WAF、主机IDS等常见安全设备的报警并知道如何处理。
3）熟悉安全应急响应的流程及方法。
4）了解各类安全程序及设备的原理，构建企业自身的安全监控体系。

讲师： HRay、Rozero、LS

白帽子提问:有没有啥开源的主机安全监控系统?

ossec、ossim，收费的就多了.....

讲师： HRay、Rozero、LS

安全运维体系建设的难点在哪里？如何解决？

京安小妹

安全运维是基于传统的网络、主机、终端、视频等运维工作的，从传统运维中获取原始的数据与信息是构建安全运维体系的基本要素。----信息统一搜集、安全运维告警中心，也就是建设的难点。
传统很多商业软件或供应商会提供很多解决方案，例如威胁情报平台、SIEM（security information and event management安全信息和事件管理平台）
但这些打包的商业平台，很多时候落地会水土不服需要安全人员进行二次开发。
而这里又有一个难点就是各方面的信息如何准确收集（网络异常流量、VPN\OA异常登录、内网非法接入），
通用解决方法就是：了解网络、数据的流转过程，在源或者末端进行搜集分析。

比较普遍的一个就是推动工作吧，我记着刚开始做推动工作的时候，经常被研发反馈的一些情况就觉得这事不能做了，后来回头仔细想想还是有解决办法的，然后再去找研发沟通，这么一来相当于否定了自己之前的说法，对于研发来说也会感觉你不太专业。随着经验增加你的思路会越来越多，逐渐改善这类情况，但是对于经验不足的同学来说，一定要记住不要先把话说死，你要是暂时没啥思路就说回去想想再给反馈，实在想不出来就拉上几个人一起讨论，你得知道你是要对结果负责的，有问题多想着去解决问题，不要轻易放弃。还有些是推动的研发自身的问题，不太想干活之类的，在一个办公区的比较容易些，我一般会过去坐他旁边盯着弄，不在一个地方的就天天打电话催。另外还有资源问题，比如我们研发本来就被项目把时间压的很紧了，又是对公司很重要的项目，这种就需要你尽量把自己能做的事都做了，实在做不了的只能先延期，毕竟要以公司业务为主。我们这种创业公司一般资金比较紧张，没钱买外面的安全产品，可以做些适合企业自身情况的精简替代品，不一定非要高大上，有作用就行。

1、难点在于要解决什么现实问题，从建设的角度来说，难点不在于具体的技术细节。而在于如何将安全能力有效传递给其他部门。做到不给业务添堵，并把安全做好。
2、其次就是要有足够的数据，才可以监控到整体安全状况，当出现安全事故时，可以整合上下文完成事件追溯及日常监控。
3、安全建设不要眉毛胡子一把抓，需要着重建设安全的监控及处理能力。通过监控来发现建设中存在的不合规的问题，并加以解决。

讲师： HRay、Rozero、LS

是否有成熟的工具推荐?

京安小妹

freeipa：ssh认证统一管理
巡风：一款适用于企业内网的漏洞快速应急、巡航扫描系统
opencanary：低交互蜜罐
suricate：一款开源IDS
clamav：linux杀毒软件
rkhunter：rootkit检测工具
ossec：基于主机的入侵检测系统

常用的工具，如下：
网络数据包分析：wireshark、tcpdump
漏洞扫描工具：nmap、nessus、nexpose、awvs、openvas
主机安全安全：ossec、lynis、chkrootkit
日志分析 ： splunk、elk
编程语言：python、php、c
系统：backtrack

openvas、Wireshark、Snort/suricata、Netcat、Tcpdump、nmap、Elk stack

讲师： HRay、Rozero、LS

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文