安全小课堂第129期【企业安全建设思考】

京东安全应急响应中心 2月19日

甲方安全无小事，在不同类型、不同体量的公司做法却有所不同。但万变不离其宗，万丈高楼平地起，我们依旧需要做好基础的工作，再谈"高端"玩法。

JSRC **安全小课堂第129期**，邀请到**bloodzer0**作为讲师就**企业安全建设思考**为大家进行分享。同时感谢小伙伴们的精彩讨论。

企业安全建设涵盖的内容有哪些？

京安小妹

bloodzer0:

安全是一门含义很广的学科，信息安全、网络安全、网络空间安全等都是安全中的一个分支（最近这几个概念也被炒的有点火），有交集却也有不同。
对于甲方企业安全来说，通常又分为：安全体系（等保、合规、审计）、基础设施安全（主机、网络、终端）、应用安全（Web、移动）、业务安全（账户、交易、内容、活动）、安全运营（应急响应、安全培训）、数据安全（加密、脱敏、存储）等等，特殊的行业还会涉及iot、物联网等。不同企业在不同的发展阶段所侧重的安全点也不一致。
在上述的每一个类型中有很多子类，每个子类都有一个循序渐进的路线，比如：安全测试工作

> 安全测试一般分为定期的安全巡检、新业务/新功能上线前的安全测试，安全测试在应用安全中算是一个比较小的点。但是我们通过一定时间的安全测试，整理我们通过安全测试所发现的漏洞得出出现漏洞的原因，形成设计规范，编码规范进行推广到研发团队、产品团队，并逐步参与到产品的整个流程中，这样就无形中推动了"S-SDL"。

整体来说，安全是一条漫漫路，一步一个脚印踩扎实很重要！

从白帽子到甲方安全工程师的转型思路是什么呢？

京安小妹

bloodzer0:

目前很多甲乙双方企业中的安全工程师大部分都是由白帽子转型过来的，但是由于漏洞挖掘与甲方安全建设还是存在很大的差异，所以我们在转型的时候需要做好几件事：

1. 做自己擅长的事情：安全测试（漏洞挖掘），这里的安全测试需 要更全面的进行，因为甲方安全中需要防御所有的面，而不是一个点。
2. 通过问题看本质：如果业务系统中长期存在SQL注入、XSS，那么说明研发对于安全的认知还不够，我们这个时候需要协助来推动安全编码规范。很大程度上，推动安全编码规范是很难的事情，那么我们可以转换思路来推动安全开发红线；如果服务器长期被入侵、被挖矿，那么说明运维对于服务器的安全做的不够好，这个时候我们可以帮助运维一起推动服务器安全基线等。
3. 初期要做的：定好宗旨，与"老板"(这里的老板要能够直接或间接决定公司整体安全建设的路线路)确定好短中长期目标，这里的每一个目标我们都需要预留出足够的时间，要考虑到各种可能影响目标达成的因素。
4. 3+1：这里的3指的是"互联网企业安全高级指南"中第三章提到的3张表。这里的1指的是"权限梳理"，如果前期你通过漏洞挖掘、渗透测试没有发现公司的业务系统存在很大的安全隐患，那么我们这个时候可以来做这件事，推动权限梳理需要跟领导报备再进行，这是一个不能立竿见影的安全项目，但是做好它我们能够发现很多企业中可能存在的风险点，重点关注如下几个方面：

   （1）从员工的角度出发：每个员工拥有哪些权限？每个拥有的权限是否合理？

   （2）从业务系统的角度出发：业务系统的用户群体是什么？ACL是否正确？拥有系统权限的是哪些人？（这个地方可以与第一个角度进行交叉对比，查看两者是否有"漏点"）

   （3）从权限设计的角度出发：如果系统拥有超级管理员、管理员、审核员、客服4个角色，那么是否存在越权操作的角色用户？

讲师

在企业安全建设中，需要安全工程师具备哪些技能和如何去成长？

京安小妹

bloodzer0:

关于技能：（聂总军分享）

链接：https://pan.baidu.com/s/1AsxnamJASlis1aGz6OdwIA

提取码：x21X

任何人都不是一开始就精通各种技能，我们应该做的就是找对合理的路线并坚持学习下去，终有一天能够学有所成，当然有一个合适的学习计划很重要；

1. 选择适合自己的路：甲方企业安全在第一个问题回答了有很多分类，每个人也有自己擅长的地方，如果你对攻防技术很感兴趣，那么你可以朝着红蓝对抗的方向走；如果你对操作系统比较敏感也可以努力钻研主机安全、应急响应等。（兴趣很大程度上能支撑你在这个方向上走下去）
2. 学习的方式：阅读文档，关于甲方安全有太多太多的资料可以供我们去学习，我们可以在低一点的基础上找到这些文档进入深入解读积累成为自己的知识；参加沙龙或讲座，对于峰会、沙龙或讲座可以优先确定是否有自己喜欢的议题，专心去聆听分享者的讲诉，一次会议能够真正学到1-3个议题的精髓就足够了；互相交流，不同公司在不同安全上可能有不同，但万变不离其宗解决问题的本质思路也行还是一致的，所以适当与同行业甚至跨行业的安全朋友进行探讨也是快速学习的方式。（补充一下，针对文档，大家一定要养成合理归纳整理，需要的时候翻出来看看非常有益处）
3. 纸上得来终觉浅，绝知此事要躬行：实战经验，资料看的再多，与人争论的口若悬河都不如自己实战一次，安全项目只有在推动过程中不断从一个坑爬到另外一个坑，我们的技能才能快速成长。不要怕踩坑，如果你的项目推动的一帆风顺，也许是你没有进行充分的问题预估.
4. 平台选择：大平台与小平台各有优势，也各有劣势。大平台的优势是视野以及你所能遇到的流量、场景都不是小公司能给你的；小公司的优势是你能接触到面要广一些，但是容易杂而不精，但是如果你能合理分配你的精力也是没有问题的。

讲师

在企业中，如何将一个安全项目落地?

京安小妹

bloodzer0:

国内大部分企业推动安全项目是合规驱动和事件驱动，那么我们在推动安全项目的过程中应该如何来做。首先要明白几个特性：

为什么这么做？背景（我们遇到了什么样的困难导致我们要这么做），做了以后的好处是什么？目标谁来做，怎么做，什么时间做？过程做这件事可能遇到的问题有哪些？预估风险是否是最优的解决案？如果不是行业最优解决方案，我们为什么要选择这个方案？其次我们在推动过程中要注意2个细节，做好项目预案后，要将整个项目的推动过程拆分成多个阶段，定好每个阶段的时间节点，每个阶段的时间节点需要预留足够的时间。在每一个时间节点进行总结会议，上一阶段的完成情况，如果未完成原因是什么？本阶段的预期等。

（举个栗子）推动主机入侵检测项目：

1. 背景：多次遇到了主机被入侵挖矿的安全事件；
2. 目标：及时发现主机被攻击或被入侵；
3.过程;

> 调研：
> 调研内容：功能、对系统的性能影响、安全性、部署难易程度、管理难易程度、可扩展性
> 调研产品：开源（ossec、wazuh、osquery、驭龙）、商业（安骑士）
> 部署方式：自动化部署实现方案。
> 谁来部署：安全负责入侵检测服务端，服务器系统初始化时部署入侵检测客户端。
> 时间节点：测试-->测试环境-->非核心业务环境-->核心业务环境（根据服务器数量来确定时间节点）

4. 风险预估：客户端对服务器系统性能产生影响如何快速卸载；误报太多如何处理。

在推动安全项目与其他业务项目不一样的是，部分安全项目会对公司的业务系统产生影响，比如：上WAF需要考虑对业务造成的延时，WAF能承受的最大访问量；扫描器需要考虑的脏数据，部分扫描行为会造成Dos的效果等。

讲师

对于开源和商业产品，我们该如何选择？

京安小妹

bloodzer0:

一句话总结来说就是：有钱买产品、没钱就开源、人少直接用，人多自己改。很多人存在误区：开源挺好的，节约钱不用找老板要预算，其实开源有很多问题：

1. 安全性：安全开源产品本身的安全性，我们在使用开源产品的时候大部分情况下都是没有对产品本身进行安全性审核；
2. 持续维护：目前国内开源产品呈现出一个比较严重问题就是没有长时间维护，如果我们使用国内的开源产品，后续还是需要二次开发。
3. 成本高：成本=采购成本+运维成本+更新成本，开源产品没有采购成本，但是运维成本与更新成本远远高于商业产品；
4. 兼容性：我们可能选择了不止一款开源产品，如何把这些安全产品集成起来是我们头疼的事情；

对于商业产品，我保持以下的态度目前公司所存在的风险急需一款产品来解决；能带来直接或间接的安全能力提升。这都是针对安全经费并不充足，业内还有一种驱动安全项目的为消费型驱动，他们不存在这些，买就好！

借用一下我的安全座右铭:

安全就像是癌症一样，对二者而言及早发现问题均能减少其造成的破坏，但能否找到完美解决方案是个疑问。

--鲁迪-齐兰尼

讲师

互动问答环节：

1. 自己开发，摸石头过河的过程可以提高团队的安全积累，这些往往不少看些PPT就学会的；采购商业产品就直接用了，当然最终的目的都是解决安全问题，这中间怎么平衡？

你们是怎么做的?

讲师:我最后有一句提到了：有钱就买公司在没有达到一定规模的时候自研其实就是扯淡，如果领导给经费就买，不给就看看开源能不能用，实在不能用，还是需要回到申请经费的路上。

2.在甲方想要从工程师晋升成管理人员有什么可以关注得地方么，该怎么做?

讲师:工程师晋升管理人员，我觉得快捷方式就是考证。

3.有哪些证比较好呢?

讲师:cisp，cissp，cism（递进关系）。

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，点击菜单栏进入“安全小课堂”即可浏览。

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

文章已于2019-02-19修改