安全小课堂第六十九期【企业安全基础框架】

京东安全应急响应中心 2017-08-14

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 **安全小课堂第六十九期**，邀请两位老师分享企业安全基础框架相关知识，本期小课堂邀请到了HRay、**Rootsecurity**老师进行分享。同时感谢JSRC白帽子们的精彩讨论。

对于企业来说网络安全的基础框架包含哪些模块?

京安小妹

1）端口对外开放的管控（很重要）
2）主机系统，web系统授权的集中化
3）webshell监控
4）bash监控
5）WAF（没钱买的话用类似百度云加速这种免费的云waf就好）
6）漏洞扫描系统
7）DDOS防护（没钱买设备依然可以使用云加速这种免费的云waf）
其实还有好多事情可以做，不过题目既然是基础，就不扩展太多了

我认为企业网络安全整体包含四大块：
1.基础架构的安全
2.应用与交付安全
3.业务安全
4.建立信息安全管理体系（设计流程、整体安全策略）。

讲师： HRay、Rootsecurity

这些模块的作用分别是什么？

京安小妹

1.基础架构的安全
其中包含：IDC机房、生产网络里面的各种链路和设备、服务器、大量的服务端程序和中间件、数据库等。偏运维方向的会比较多，跟漏洞扫描、打补丁、ACL管理、安全配置、主机入侵检测等这些事情关联比较多。
2.应用与交付安全
其中包含：对各个事业部、业务线以及其他自研的产品进行应用层面的安全评估、代码审计、渗透测试、代码框架的安全功能等。
3.业务安全 其中包含：业务风控系统、征信系统、账号安全、反爬虫、反刷单、反欺诈、反垃圾信息等，像部分游戏行业还会涉及反作弊、反外挂等等，能有效打击部分线上/线下黑（灰）色产业链。
4.信息安全体系/管理（设计流程、整体安全策略）。

1）企业的内网一般会充斥着大量的安全问题，甚至好多是可以一步入侵的，比如struts2，redis未授权访问等等，如果端口完全暴露会很容易被搞，所以端口对外开放的管控很重要。
2）企业经常会有员工变动，如果授权分散，就会出现离职员工权限清理不及时的问题，还有就是集中化授权可以让授权更可控。
3）企业被入侵总要有些方式知道自己被搞，webshell的监控就是其中一种比较基础的。
4）同上，bash监控也是知道自己是否被搞的一种方法，另外也方便检查某些文件无缘无故丢了是不是运维的误操作。
5）企业往往无法避免自己会出现web层面的漏洞，有了waf，虽然存在被绕过的可能，但还是极大的提升了攻击成本，同时避免无脑的扫描。
6）漏洞扫描是检测企业自身问题必不可少的东西。
7）安全是要保证业务正常稳定运行的，随随便便被几个G的DDOS就打挂肯定也是不行的。

讲师： HRay、Rootsecurity

要搭建这样的框架需要工程师具备什么样的能力?

京安小妹

企业安全人员比较多的话，做的事一般负责一个方向即可，但是会强调深度，每个方向都会有不同要求，这个不细说了，看各个企业的招聘说明即可。如果安全人员只有1-2个人的话，我个人觉得至少需要以下能力：

1）熟悉各种常见的攻击方法并知道如何防御。

2）了解各类安全程序及设备的原理。

3）有比较丰富的安全应急响应经验。

4）可以独立搭建部署大多数系统（没钱没人的情况下需要你独自去搭建一些开源系统）。

5）具备一定的开发能力（不要求太强，但是有些小脚本肯定要自己写的，不能啥东西都找开发去做）。

6）可以与其他人比较好的交流（这点容易被忽略，人少的情况下做事都要自己去推动，光有技术不懂交流肯定是不行的）。

1.Layer2-Layer7 从数据链路层到应用层每一层都拥有完整的安全设计。

2.对所有服务器、终端、办公网PC、移动设备具有统一集中的安全监测及防护能力。

3.应用层面细粒度控制，对所有自研的产品具有自主的评估和修补能力。

4.核心全流量入侵检测能力。

5.严重/高危无死角1天发现并解决漏洞。

6.对业务安全形成自己的风控及安全管理方法论。

7.引入第三方安服团队。

讲师： HRay、Rootsecurity

搭建企业网络安全基础框架的过程中主要会遇到的问题有哪些？如何解决？

京安小妹

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。

甲方可能存在几类人，第一类是对安全行业涉猎不深，还停留在原始执念阶段，使劲堆防火墙、IDS、IPS之类的硬件设备，第二类是“业务怎么样与我无关”，只要不出安全问题，业务死了都无所谓。这两种从表面看都属于一类，但本质不同，第二类可能只是口头唱安全重要，但是心里还是会妥协。反过来看那些说宁可业务死也要做安全的观点的初衷是什么呢，也许你猜到了，怕担责！因为业务死了安全团队不用担责，他们可以说：“你看安全不是没出问题吗！”这固然是一种保护自己的方法，但我认为安全的本质还是要为业务服务，如果业务死了，即使安全做的再好也没有价值，更准确一点说，安全需要为业务量身定制。安全做的不好的表现除了无视业务死活，还包括用户体验大打折扣，产品竞争力下降，影响工作效率的内部流程增加。
那么到底哪些必须妥协，哪些必须坚守呢？我认为像严重/高危漏洞，有明显的利用场景，不能妥协。但对于不疼不痒的漏洞，表现为开发周期长，受众面小，边缘性的功能和产品可以考虑酌情妥协。

讲师： HRay、Rootsecurity

白帽子提问:webshell监控这个有啥开源的系统么?

最早我记得有一款开源出来的系统叫falcon

讲师： HRay、Rootsecurity

在基础框架的基础上要进一步做好企业的网络安全，主要的工作方向有哪些?

京安小妹

我认为主要工作方向有两个：
1.纵深防御。
2.分阶段安全体系建设。
纵深防御这个词语在安全圈已经被写烂了，但凡是个安全产品都说自己有态势感知和纵深防御的体系，但是实际并没有什么卵用。甲方需要根据资深业务来整合和利用资源，但是无论如何都需要有一个安全底线，这个安全底线在生产域一般可以总结归纳为：
入侵者能随意操作数据库（包括：dump,os-shell,sql-shell等敏感操作）
渗透达到了应用层（得到了shell，无论是否交互，是web还是操作系统）
企业在安全体系建设实际上是一个从0到1的过程，很多安全从业人员现在充当的角色还是救火人员，并没有接入业务，发生安全事件后永远处于被动状态。
首先安全人员在上任后，应立马熟悉和梳理现有业务，保证在你上任之后上线的业务系统都是安全的，其次要清理“灰色地带”，这里所谓的灰色地带一般是指资产管理（CMDB）没有统计到的边缘业务系统，或者在边缘DMZ区域内的第三方或外包开发的系统，这些系统往往容易存在系统弱口令，应用弱口令，SQL注入，文件上传点，命令执行等问题。
建立应急响应能力，比如SRC等。

1）数据安全，安全工作大多数做的事其实还是保证企业的数据不被窃取，所以如果重要的数据可以妥善保管，一定是大有好处的。
2）业务安全，面对大量的刷单，扫号，薅羊毛，业务安全必不可少。
3）推动企业中各种东西部署的规范化，这个对运维和安全都很重要，规范的话可以比较方便的根据企业自身情况做出适合自己的一些安全监控，还可以在默认配置中加上一些安全相关的参数。
4）多通过技术手段保证或协助判断实现安全规范的实施。

讲师： HRay、Rootsecurity

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。

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