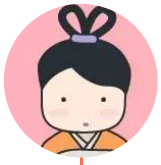
论安全漏洞响应机制扩展

2016-03-25 京东安全应急响应中心

“天下武功,唯快不破”。安全响应中心接到漏洞后，我们不能让它沉睡在系统中，应该保证速度，也就是快速的去响应，才能保证白帽子所提交的漏洞发挥最大价值。接下来一步，将白帽子挖洞思路逐步整理并融合于企业安全评估与渗透的方法中去，提升我们的工作效率。今天我们来谈谈安全漏洞响应机制的扩展。

本期安全小课堂非常荣幸的邀请到了来自百度安全应急响应中心的byteway、唯品会安全应急响应中心的终极修炼师、联想安全应急响应中心的艾惠！这三家公司在互联网、电商和传统行业分别都非常有代表性。大家的掌声👋、鲜花💖、口哨声□在哪里~~

1



豌豆妹

大家是如何看待企业的安全工作建设呢？

我就是叫小强

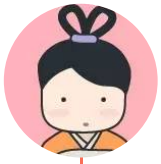
“上医治未病,中医治欲病,下医治已病”。甲方企业推动安全建设的角度，就需要看安全工作者是站在医生的角度还是金正恩的角度了。应急这个话题已经是在已病啦。而RD常会以产品方面的理由当作修复进度滞后的借口。说得通俗点，可以理解为生病了，咱们找到病根进行治疗，然后在平时中多注意，多强身健体，以防下一次疾病。而不是以任何的借口来影响修复的进度。

狂拽炫酷屌炸天的我

我个人觉得安全响应中心不仅仅是接报漏洞，还需要帮助内部提升安全质量，分为两方

面：一个是被动，一个是主动。被动方面，比如说进行针对性的培训，加强规范。需要明确的是，安全团队是在帮助业务部门防范风险；主动方面，应该是我们增加的那些检测机制，例如在上线流程，或waf中增加策略，可以直接进行自动化检测。漏洞的处理是一个方面，对于内部的项目上线筛查可能比后续更重要，通过需求评审，架构评审，安全评审等来筛选项目是否够上线的条件。上线前充分筛查，上线后出现问题，基本都可控。另外，上线流程过程中可以开发一些黑盒、白盒扫描工具，提供给开发人员，让开发人员去自查，如果有问题再找安全部门，这样开发人员也会对安全越来越了解。只要解决开发部门的自我驱动，所有问题都迎刃而解。

2



豌豆妹

安全响应机制整个流程的结束点在哪儿呢？

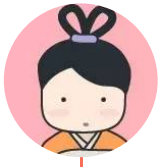
我是小新

白帽子提交漏洞，企业应该按照白帽子提供的方法结合自己的业务去查是否还有类似的问题，白帽子的漏洞提交只是事件处理的开始。处理完相同类型的漏洞，才能算是结束。

我就是叫小强

我理解的是工作从短信开始，反思结束□~一般短信来了，都是高危报警，所以是整个事情的开端， 反思是漏洞修完后RD&QA&安全能力方面的总结！

3



豌豆妹

来说说跨部门协作配合修复漏洞的“爱恨情仇”吧~

小花就是我

白帽子提交漏洞后，我们首先会验证漏洞是否确实存在，接下来我们会判断业务影响程度、业务范围，并且把这个事件报告给RD&OPS去修复，有些漏洞不一定能及时修复。但这不会影响我们对漏洞的评级。在企业中，越大的企业越会出现漏洞修复推进困难的情况。

我就是叫小强

我理解，“提升安全能力”不在应急止损的关注范围内，可以包括在后续安全建设中。跨部门修复方面主要分“产品线重视自觉寻求帮助”和 “上级推动” 两类，有流程系统做定期邮件抄上级进行提醒。

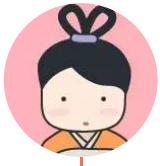
狂拽炫酷屌炸天的我

还有就是7天修复率，定制漏洞修复事件dead line，如果不修，逐级上报。

我是小新

此外，还可制定不同级别漏洞对应不同修复时间的要求，严格执行考核。超期系统自动邮件抄处理人的上一级领导，时间越长，抄送级别越高，直到超送到技术副总裁。

4



豌豆妹

一个业务部门如果多次出现同类型问题，有相应的响应机制么？

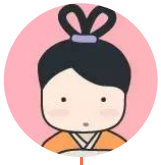
狂拽炫酷屌炸天的我

需要看是什么类型问题，是工作态度问题还是技术能力不够，如果是前者要找他们leader去沟通，如果是后者，安全部门需要组织交流培训，提升业务部门的安全意识和技术能力。

我是小新

对！需要定期培训，不定期share，我们内部就有一个信息安全月刊。

5



豌豆妹

大家来分享下各自的安全应急响应机制呗~□

小花就是我

建立安全接口人，协助产品线培养免疫力。阶梯性的做安全培训，后续让产品线他们自己重视培训，提升安全意识与能力。

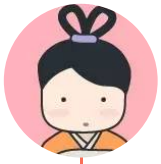
狂拽炫酷屌炸天的我

高危漏洞我们会及时打电话通知修复，同时@安全接口人、业务部门老大；然后每月的月报会有7天漏洞修复率，抄送给每个业务部门。

我就是叫小强

补充一句，高危漏洞24个小时内修复！！！

6

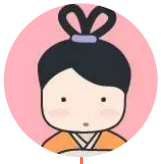


豌豆妹

后续我们做个安全质量提升最佳实践联盟，大家觉得是否可行？

狂拽炫酷屌炸天的我

表示支持。这个联盟可以主要讨论我们通过响应中心沉淀下来的主动防御漏洞方法，提前规避风险。例如，xss防御，大家都说用现成的防御函数，为什么还会有这么多有问题的，大家都可以一起集中讨论。



豌豆妹

大家讨论激烈，超乎异常啊！非常感谢大家参加京东安全应急响应中心组织的安全小课堂第三期，撒花~欢呼~感谢三位嘉宾和各位核心白帽子的积极参与！

我就是叫小强

飞吻~~□□□期待下一期！

JSRC http://security.jd.com/

长按识别左侧二维码，关注我们