# 某某安全应急响应中心

## 概念介绍

**安全应急响应中心（SRC, Security Response Center）**，是企业用于对外接收来自用户发现并报告的产品缺陷的站点。一般起着对外发布企业突发安全事件处理动态，作为企业与热心用户以及安全研究人员沟通反馈的平台以及对外发布企业信息安全团队研究成果的重要作用。 目前安全应急响应中心主要有两种实现方式：

**1、 漏洞报告平台。**漏洞报告平台是指由独立的第三方公司或机构成立综合性的“安全应急响应中心”。国内补天平台、漏洞盒子平台，以及据此衍生的Sobug众测平台等均属于该模式。外部报告者注册对应漏洞报告平台选择对应的厂商进行报送，接着该第三方机构会发送邮件提示相关厂商确认处理。这种方法的缺陷十分明显。厂商的历史漏洞信息完全暴露给第三方机构，报告中涉及的企业内部大量敏感信息因此外泄丧失私密性。

**2、 xSRC模式。**xSRC模式是指：企业自己分配工程师开发属于自身的安全应急响应中心，制定自己的漏洞收集和披露计划。目前包括Google、Microsoft以及腾讯、阿里巴巴、百度等，均成立了自己的安全应急响应中心，对外收集并处理安全研究员报送的漏洞报告。使用这种模式，企业在漏洞的收集和披露过程中完全掌控了主动性，拥有良好的私密性和可定制性。

## 为什么会有安全响应中心？

基于企业为保护重要或海量的数据不被黑客篡改或盗取，对于有一定规模的企业陆续成立了内部的安全部门，这称为正向防御。但还会有一些未知风险是正向防御不能覆盖的，如何弥补这些空白？如何从逆向建立防御系统？由于计算机的产生与早期发展，国外快于国内，所以，在借鉴了国外先进经验之后，中国企业成立了自己的安全响应中心security response center，简称SRC，作为企业回收外部风险的入口。同时SRC还扮演着安全部门与行业内安全从业人员交流平台的角色，通过这个平台，企业建立了与安全人才的联系，为企业的人才储备作出一定贡献。白帽子，本企业以外的安全从业人员（正面的黑客），可以通过SRC这样的渠道向企业提交自己发现的安全漏洞，并获得企业给予的一定的物质与精神的奖励。简而言之，安全响应中心的初衷是企业集结分散在社会中的技术资源来保障企业安全的一种防御手段。

## 重要性和必要性

近年来黑客攻击频发，企业信息安全已经愈来愈受到重视。腾讯安全平台部应用运维安全中心总监lakehu先生在其发布的研究论文《企业安全应急响应中心建设理论与实践》中提到，“大型企业的业务模式多，涉及的产品也多，特别是互联网业务讲究小步快跑敏捷迭代，往往忽视了安全检查或者来不及进行细致的安全检查，同时安全系统本身是程序也会存在各种遗漏，因为互联网业务的在线特性，使得互联网的人都能够接触到，相对于传统业务被攻击面扩大，所以更容易被善意的、恶意的或者无意的人发现漏洞——如果漏洞被利用或者在黑市交易，对企业和用户是极大危害的”。

纵观国内外，Google、微软、阿里巴巴、腾讯、小米、网易等知名互联网公司都已经建立各自的应急响应中心，并在推出以后取得了良好的效果，对企业安全有了巨大的协调和推动作用。

## 法律法规要求

《中华人民共和国网络安全法》

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、

举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

《网络产品安全漏洞管理规定》

第五条 网络产品提供者、网络运营者和网络产品安全漏洞收集平台应当建立健全网络产品安全漏洞信息接收渠道并保持畅通，留存网络产品安全漏洞信息接收日志不少于6个月。

第六条 鼓励相关组织和个人向网络产品提供者通报其产品存在的安全漏洞。

第七条 鼓励网络产品提供者建立所提供网络产品安全漏洞奖励机制，对发现并通报所提供网络产品安全漏洞的组织或者个人给予奖励。

## 网络安全行业现状

安全行业内有一种称呼叫“脚本小子”，指初入网络安全行业，渗透测试完全依赖脚本的一类人。像最近的Confluence漏洞，能够直接获取服务器权限。而利用脚本已经在GitHub上有公开。每当有这样的漏洞出现的时候就很容易被脚本小子到处扫描。

之前的网络安全爱好者，当前兴起的渗透测试培训班的学员，一般老师在教授东西的时候都会说明让大家不要去搞破坏，可以去给SRC提漏洞。

在这个阶段，很需要认可感与成就感，积极性极高、正义感爆棚、精力充沛。情绪化程度高，破坏力强。企业建立SRC之后可以给这群爱好者一个平台，企业付出一点经济利益，收获数量客观的白帽子。虽然高手不多，但胜在数量多，覆盖面广，可以检查暴露明显的漏洞。

隐藏比较深的漏洞，SRC一般会与乙方漏洞平台合作，邀请高手来进行渗透测试，进行深入的漏洞挖掘。

真实的黑客攻击的技术手段就是以上两种情况，即深入的漏洞挖掘来突破防御或大面积的测试资产来找到薄弱点突破。

真实攻击中社工等安全意识方面的攻击手段，这种攻击的防御依赖安全意识培训，大家安全意识的提高。

## 建设模式介绍

目前，“漏洞报告平台”模式在实现过程中由于操作运营的规范问题，外加越来越多的鱼龙混杂的第三方企业和机构的介入，甚至出现了漏洞报告平台泄漏企业敏感信息从而导致企业因此被攻击的案例。大多数互联网企业对“漏洞报告平台”既“爱”又“恨”，典型的如乌云平台。

因此，出于私密性和可定制性的考虑，大多数互联网企业均倾向于选择“xSRC”模式。作为互联网企业安全防护体系中用户所能直接接触到的门面，同时也作为协调企业各部门对安全事件做出及时积极响应的工作中心，越来越多的企业意识到，建立安全应急响应中心和建立产品交流论坛、博客、WIKI等站点同等重要。

## 其他企业SRC一览



## SRC成立申请

鉴于法律合规及某某数据保护的安全需求，结合实际业务场景，电商模式、对接抖音、流量及曝光巨大、工厂众多，另外考虑到某某在服装供应链行业的头部地位、品牌声誉，以及资本市场的好感度。迎合要求，申请成立安全应急响应中心。建设方案如下。

## 建设方案

某某安全应急响应中心建设采用web站点方案，XSRC模式，使用腾讯开源SRC建站软件，可直接搭建使用。代码开源，可根据需求二次开发。网站代码经过腾讯安全审核，数据存在某某服务器本地，安全可靠。

## 运营方案

结合某某实际业务场景，参考电商行业及工厂行业的SRC建设运营方案及奖励标准，计划运营方案如下

1. SRC声明基本原则，保护用户信息，规定安全测试规范。
2. SRC声明某某资产范围、业务范围、漏洞范围。
3. SRC声明处理流程，一个工作日内确认漏洞，三个工作日内给出评分。
4. SRC声明评分标准、漏洞等级、贡献值及对应奖励
5. SRC展示提交者榜单与英雄称号
6. SRC每月第一个工作日发放上月兑换礼品与现金。
7. 计划SRC每年举办一次活动，时间长度为半个月，期间奖励翻倍。
8. 计划SRC成立之后与乙方厂商合作推广一次，计划为安全工作建设一段时间之后，具体时间待定

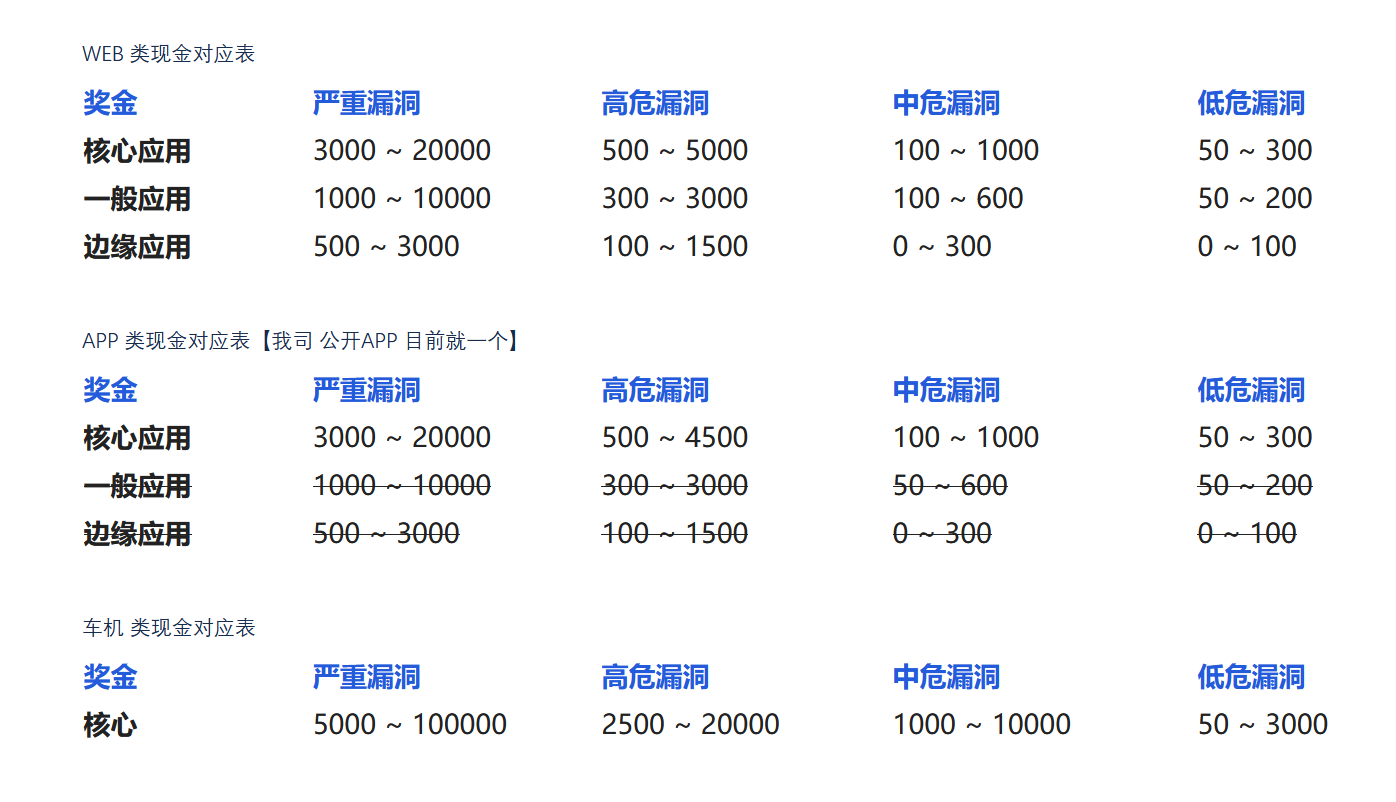
## 奖励标准

参考其他SRC奖励标准，制定某某奖励标准如下

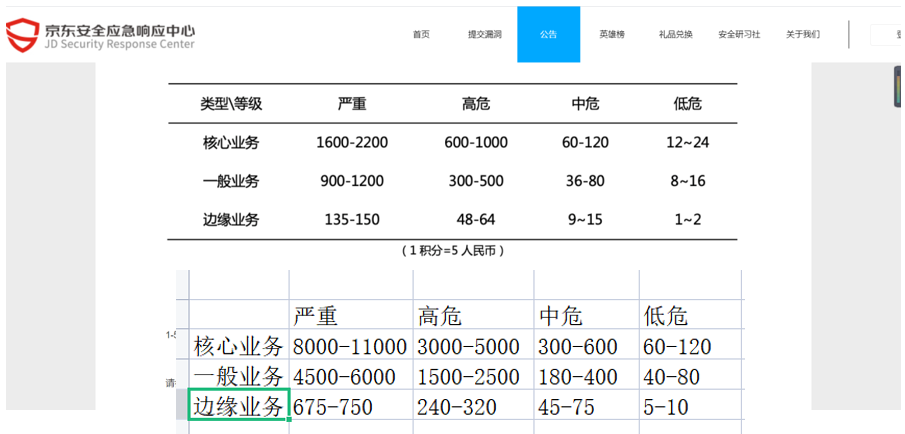
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SRC 贡献值体系 | | | | |
| 危害分级 | 积分 | 现金奖励范围（单位： 元） | | |
| 边缘 | 重点 | 核心 |
| 低 | 1-2 | 10-20 | 20- 40 | 30- 60 |
| 中 | 3-5 | 120- 200 | 150-250 | 180-300 |
| 高 | 6-8 | 420-560 | 480-640 | 540-720 |
| 严重 | 9- 10 | 900-1000 | 1800-2000 | 2700- 3000 |

其他企业奖励标准如下

理想汽车SRC



京东SRC



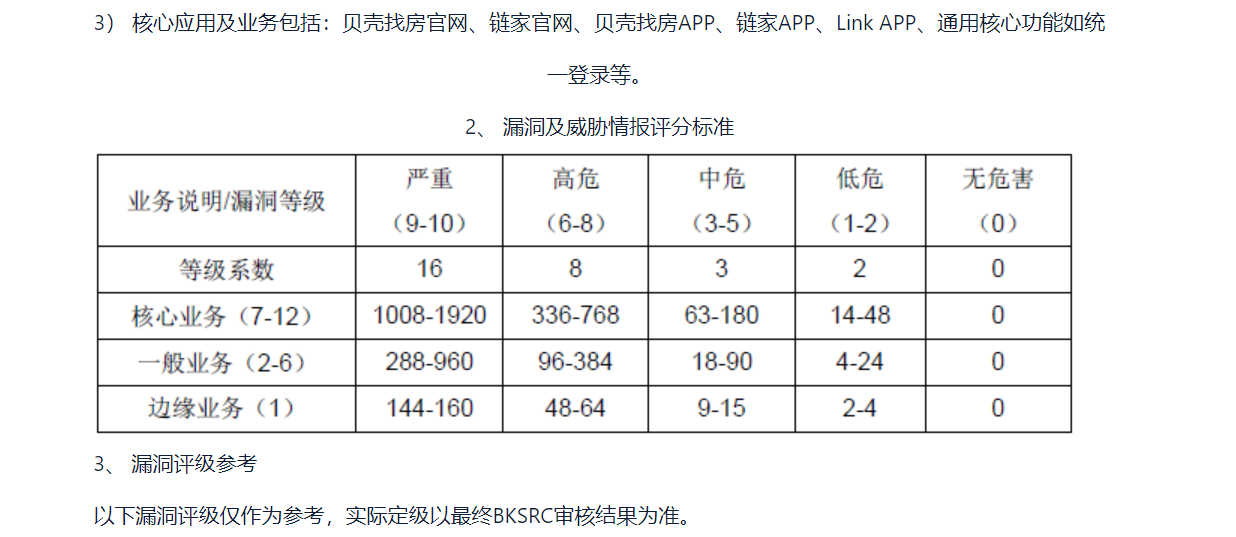
小米SRC



中通SRC



链家SRC



## 预算规划

按照某某奖励标准，单个严重漏洞奖励总和为6000元，因此首次申请6万元预算。

参考其他厂商及自己的实际情况，年度预算为30万。

奖励中可以放一些自己 产品 的产品类目，比如西服，流行服饰，支持定制的高端一些的服装产品，白帽子可以兑换之后自己穿，或者送长辈，送亲戚朋友。这样可以节省一部分现金开支。