安全运营中心

最佳实践

产品文档

腾讯云

文档目录

最佳实践
数据泄露监测
数据泄露相关说明

最近更新时间：2023-08-29 15:59:14

定义

数据泄露指受保护或机密数据可能被未经授权的人查看、偷窃或使用。由于企业业务性质及开发制度等原因，互联网公司一般会涉及较多的版本变更，且大部分互联网企业内部崇尚开源文化，开放的同时，也为数据泄露事件埋下隐患。

适用对象

业务上云的开发者、运维工程师及安全领域初级学者。
业务运行云上且对数据泄露较关注的企业。

常见分类

以近几年影响较大的几个数据泄露事件为例，从泄露渠道上进行以下分类：
Github 代码类：
数据泄露原因：由于人为有意或无意的上传了包含企业内部敏感信息的代码到 Github 网站，导致被外部攻击者获取利用进行入侵行为。
案例：某大型二次元网站后台工程源代码被上传至 Github。
网站入侵类：
数据泄露原因：由于网站或服务平台、App 等存在漏洞遭受攻击，导致数据泄露丢失。
案例：某大型技术社区网站600万用户信息泄露。
网络黑市交易类：
数据泄露原因：二手泄露渠道指在地下交易市场售卖和交易的数据泄露事件，其中数据来源渠道可能会有很多种，例如，通过雇佣黑客社工获取数据服务器权限，或通过内部暗箱操作获取内部数据等。这里的数据泄露事件往往以盈利为目的，将数据在网络黑市渠道进行发布和售卖。
案例：国内某知名酒店住房数据泄露事件。
合作商接口调用类：
数据泄露原因：由于合作商接口调用内部数据没有做好安全防护措施或监测，导致敏感数据通过合作商渠道泄露到

外部。可能由于本身技术问题导致数据泄露，也可能非法将这部分数据进行他用。
案例：某分析公司以不正当方式获取5000万 Facebook 用户个人信息。

产生原因

数据泄露产生的根本原因可以总结为以下两种：
技术方面：企业对数据的技术管控策略不足导致数据泄露。如果网站、平台、应用、系统存在安全问题，例如系统漏洞或配置失误、数据脱敏手段和数据加密措施缺失、异常操作审计手段缺失、敏感信息泄露发现机制缺失等，都可能导致被攻击者利用而获取到敏感数据。
管理方面：数据安全管理策略或制度上缺失，使敏感数据被未授权的人访问导致数据泄露。由于开发人员或实习员工安全意识薄弱、或缺乏对合作商使用数据的约束或限制措施等，导致未授权数据公开或被非法滥用。

解决方案

如果企业建立了敏感信息泄露监测体系，在出现泄露事件后能通过技术手段快速应对并积极开展自查修复，在黑客入侵之前进行整改和加固防御，可以规避各类不必要的隐性风险，将损失降到最低。上文提到了 四种主流的数据泄露事件 风险，针对其中比较典型且危害较大的 Github 代码泄露和黑市数据交易这两种行为进行分析，我们提供的技术手段和管理控制思路如下：
技术管控策略
严禁员工私自搭建代码管理工具，需使用公司统一授权的代码管理工具（Github，SVN）进行代码管理。
严格管控项目代码权限，人员变动（转岗、离职）需及时回收代码权限。
大型项目使用 submodule（子模块）进行划分，对项目实行权限最小化原则。
不把代码存放在 Github、Onedrive 等外部网站。
对 Github、地下交易市场等网站进行敏感信息泄露监测，当出现敏感信息时，及时进行自查确认，避免问题扩散。
合规管理策略
制定《源代码开源安全管理》流程，代码开源需经过开源流程评估。
对合作商的接口使用范围进行约束、限制或监督审计等。
对内部员工的合同实施法律约束，采取高压线措施。

产品应用

基于 SaaS 安全运营中心对于企业安全运营的优势如下：
SaaS 化的服务省去了自身数据泄露监测系统的代码维护和服务器维护成本，使企业开发者、运维者或安全管理员将更多精力集中在规则运营上。
与云平台能够更好的整合开发、运维，将事件处理集中在一处，提高处理效率。

在误报规则的运营处理方面，SaaS 化的平台比开源系统运营更持久，基于云上用户的体验集中优化，及目前由云鼎实验室团队进行后台策略维护支持，误报问题相对较少，告警的质量相对较高。