## ****内容介绍****

本篇是系列文章的第四篇，分享一下自己对数据安全的理解。

## ****数据安全是什么****

数据安全的保护对象是公司的信息数据。信息数据有各种表现形式，如结构化数据（sql,json）及非结构化数据（图片，音频视频，office文档）。

按作用类型分类，可分为客户数据，员工数据，业务数据，财务数据，权限数据，代码数据等。当然更准确的分类方式要根据各公司自己的具体情况进行。

数据安全就是围绕着公司信息数据的安全建设工作。

## ****数据安全需求来源与演变****

其实不管是个人还是企业，都一直有数据安全的需求。只是因为科技的发展，国家法律的监管，数据安全的重要性及数据的范围定义在扩大。

拿个人来说，数据安全有财不外露、不怕贼偷就怕贼惦记的俗理。

拿企业来说，不管是古代的账房先生，还是现代企业的财务部门，都是老板极为信任的人才能担任。

但是随着互联网发展，黑灰产发展，以及国家立法的要求，个人及企业对数据保护的要求在提高，范围在扩大。而且在监管层面，对数据安全的监管检查，也慢慢变成了新的监管重点。

## ****数据安全理念演变****

2018年，第二届高峰论坛发布了《数据安全治理白皮书1.0》。

2019年，国家发布了由阿里巴巴，奇安信，公安部等联合起草的《信息安全技术—数据安全能力成熟度模型》这个国家标准。

2021年，**《中华人民共和国数据安全法》正式施行。**中共中央网络安全和信息化委员会办公室、工业和信息化部、中国人民银行也陆续出台了**《网络数据安全管理条例》《工业和信息化领域数据安全管理办法》《金融数据安全 数据安全分级指南》**等相关政策文件和行业标准。

国家后续又正式施行了《个人信息保护法》及《数据出境安全评估办法》。

2023年，由中国计算机学会计算机安全专业委员会等指导,中关村网络安全与信息化产业联盟数据安全治理专业委员会等主编,光大科技及多家产学研机构参与编撰的《数据安全治理白皮书5.0》正式发布。

## ****数据安全的建设落地****

步骤：

应急跟需求：处理应急跟公司需求

法律合规：参考通用法律法规，及行业地方等特定法规，梳理数据安全要求。

数据梳理：梳理公司所有的数据，对数据进行分类分级。建设数据发现机制跟能力

状态调研及评估：调研安全建设状态，评估建设完成度。

决策工作内容：结合数据安全调研结果，结合公司整体的建设方案，以数据安全能力模型为指导思想，来决定工作内容，内容顺序，落地方案。

整体数据安全方面的建设，可以从管理，技术，运营三个方面来做。

整体公司的数据安全管理要做好，最好有统一管理。消除数据黑洞，归属黑洞，密级黑洞。要建设数据的发现能力及价值判定能力。

技术体系上，数据有什么类型，它们对应的技术栈，技术链路是不是都覆盖了，如何适配公司自身的情况，各种类型数据的安全重点分别是什么。

运营体系上，要建设持续统一运营体系。能够可视化，实时发现数据流转，进行行为审计，进行资产梳理，监控全生命周期的安全状态。

具体到每条数据的数据安全

按数据生命周期的理念有如下简化版的落地内容

采集阶段：最小化采集，完整性校验，合法合规等。

传输阶段：传输通道加密，内容加密，两端鉴权等。

存储阶段：存储加密，介质加密，数据备份等。

使用阶段：鉴权，访问控制，脱敏，流转日志等。

加工阶段：算法安全，过程审计，结果数据分类定级。

公开阶段：脱敏，水印，合规，审计等。

销毁阶段：数据删除，匿名化处理，物理销毁等。

## ****数据安全与其他安全方面的耦合****

基础安全：

数据与数据库/数据仓库的存储对应关系

数据流转的基础组件顺序

办公安全：

安全办公，内鬼行为的审计及发现

应用安全：

应用的数据调用关系，调用权限，日志记录，全流程的串联分析

业务安全：

黑灰产分析

互联网环境下，风控模型的设计及改进

垃圾数据清洗

## ****总结****

数据安全是围绕公司信息数据的安全保护

数据安全正在成为新的监管重点

数据安全作为新兴安全领域，目前并没有很多配套工具

数据安全是全公司都应该参与的体系化的工作，它牵扯到公司全部门，而非几个部门

数据安全，与其他安全方面严重耦合。其他安全方面的问题都可能导致数据安全问题。

## ****QA****

弟弟失业中，目前在上海，正在找工作。各位大佬如果对我感兴趣的话欢迎加我VX：qinbingjie1101