OWASP 中国 Open Worldwide Application Security Project

OWASP 中国 | 北京分会 Open Worldwide Application Security Project

网安加社区

探真科技 TensorSecurity

开源网安 SECZONE GROUP

BrainAu 脑动极光 BRAINAU

数据安全合规的思与行

2024 OWASP中国安全技术论坛

全球视野下的网络安全趋势

目录
CONTENTS

01

国家法律法规基础

三法一条例

保障网络安全，维护网络空间主权和国家安全、社会公共利益。保护公民、法人和其他组织合法权益。

规范数据处理活动，保障数据安全，促进数据开发利用，维护国家主权、安全和发展利益。保护个人、组织的合法权益。

保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用。

《网络数据安全管理条例》
规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用。

02

企业内部规章制度

企业内部数据安全管理制度

集团发布数据安全理制度

一级文件:

《信息安全管理制度》-安全管理体系总则。明确信息安全部门职能范围、总体目标、工作策略、底线要求及奖惩条例。

二级文件:

《数据安全管理规定》-数据全生命周期中数据管理者、使用者的责任划分，如何根据数据场景化制定分类分级，严格区分重要数据和一般数据的性质。

《数据库安全基线管理办法》-数据库权限访问控制，重要数据备份机制，应急恢复演练以及管理人员的职业素养。

《数据运营管理流程》-数据展示、共享、提取等在流程体系中如何规避风险，根据数据重要程度和量级设立多级审批制，主导“谁生产、谁运营、谁负责”的原则。

03

合规稽查态势分析

合规稽查中的数据治理

2024年数据
安全自评估表

数据安全风险自评估

数据非法收集引发的风险

- 移动应用程序、网站权限违规调用

数据安全防护能力薄弱引发的风险

- 数据接口防护不当
- 数据库安全保障措施不健全
- 鉴权访问控制不完备
- 数据传输或存储未加密

数据处理人员违规操作引发的风险

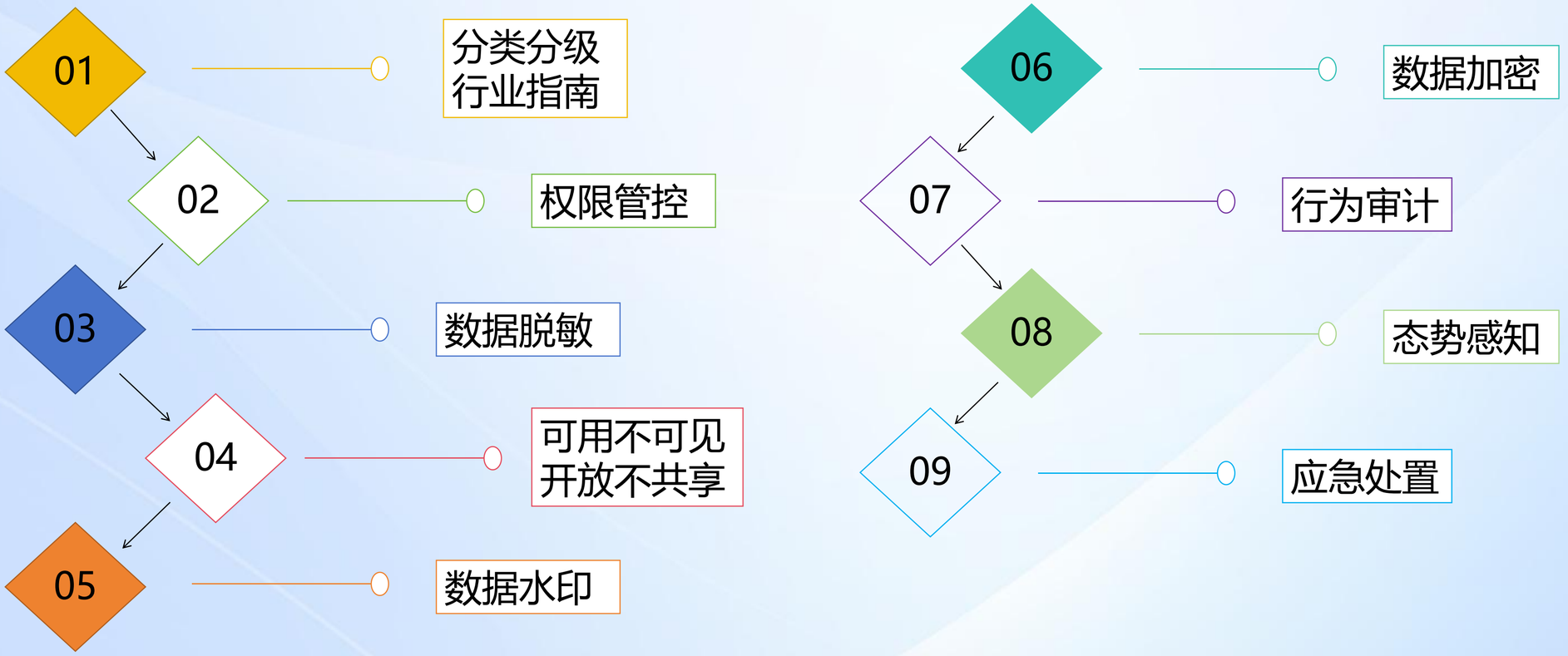
- 合作方管理不善，造成数据违规传输、泄漏
- 账号权限配置不当

数据生命周期引发的风险

- 数据采集过程
- 数据传输与存储
- 数据应用与共享

合规稽查中的数据治理

数据安全风险评估对分类分级的要求



04

数据加固应用构建

强化构建中的探索与实践

四个“统一”

一、企业内部分类分级标准以及保护措施是否统一?

*引用各行业分类分级模板时，对于同一类信息应采用同等级别划分规则

二、企业内部各业务调用加密或脱敏算法机制是否统一?

*金融、汽车、医疗、AI等行业对个人敏感信息尤为重视，
隐私信息保护意识已渗入民生的方方面面。

三、不同业务前端获取同一敏感信息是否统一管理?

*业务间对于采集同一敏感数据源不应背靠背各自管理，存储越多，隐患越大。

四、数据外发管控底线是否拉齐，数据防泄漏策略是否一致，审计标准是否统一?

*商密数据外发管控底线应根据企业数据管理制度执行统一标准，分开管理极易造成交叉传递各自逃逸。（A部门重要数据，流转至B部门被认定一般数据）

强化构建中的探索与实践

服务端数据保护措施

1.增加制度审批流程

从服务器授权直接获取导出/下载的数据，可根据重要程度，数量级，扩散范围，传输方式，操作时间等综合因素制定评估规则，加强多级审批环节。

2.数据流转态势感知

数据接口被调用时，应验证请求源是否安全。通过鉴权过滤无效访问，防患超范围或未授权窃取数据信息。

如果有能力改造系统，应针对数据库敏感字段增加标识，摸清数据流转过程，以便应对更好的保护措施。

确保系统服务上下游调用数据传输时记录全量日志，通过soc平台剧本，自动化审计排查是否存在恶意篡改或伪造数据行为的发生。

强化构建中的探索与实践

服务端数据保护措施

3.数据异地实时备份

生产数据应建立实时异地或不同机房备份的机制。

收益：数据备份可防止主数据被恶意篡改；防止数据库应用因安全漏洞被勒索病毒强行锁定；防止误操作无法还原；防止数据迁移过程中发生不可逆风险。

4.内网系统收敛

企业内部信息化系统迁移至内网访问。例如企业内部OA系统、网页邮箱、自建云盘服务等，可能含有大量的内部商密数据。

强化构建中的探索与实践

服务端数据保护措施

5.用户行为风险分析（UEBA）

*分享个人案例

（1）拉取目标生产服务器日志中当天所有操作命令，整合后排序；

操作命令(op_cmd)	计数	百分比
nvidia-smi	2221	1.90%
ceph -s	1764	1.51%
clear	1611	1.38%
dlp list	1248	1.07%
	935	0.80%
docker ps -a	884	0.76%
}	880	0.75%
ky exp list	848	0.72%
docker ps	741	0.63%
df -h	703	0.60%
export LANG=\"en_US\";export LANGU	577	0.49%
./start.sh	571	0.49%

kill	10	发送信号到进程	red
killall	4	使用进程的名称来杀死一组进程	red
mkdir	66	创建目录	red
mv	48	设置文件访问控制列表	red
mysql	19	MySQL服务器客户端工具	red
passwd	7	在当前Shell环境中从指定文件读取和执行命令，命令返回退出状态	red
poweroff	3	关闭Linux系统，关闭记录会被写入到/var/log/wtmp日志文件中	red
pvremove	5	删除一个存在的物理卷	red
rm	246	用于删除给定的文件和目录	red
ar	1	建立或修改备存文件，或是从备存文件中抽取文件	yellow
cp	180	将源文件或目录复制到目标文件或目录中	yellow
mount	5	用于挂载Linux系统外的文件	yellow
sysctl	4	时动态地修改内核的运行参数	yellow
vim	2	启动vim编辑器	yellow
clear	405	清除当前屏幕终端上的任何信息	green

（2）筛查高危操作命令，颜色区分；红色为增删改，黄色为调用工具，绿色为查看结果。重点关注红区。

（3）按照周期性统计高危命令操作频次，设定阈值，并建立监测告警机制。
稽查到异常行为告警时，立即阻断进程并强制下线当前操作账号，直至数据处理者恢复系统或服务。

强化构建中的探索与实践

客户端数据保护措施

1.办公终端标准化

办公终端至少应安装杀毒、DLP等安全防护软件。
访问内网时应加强网络准入认证以及域控认证。
内部通讯软件安装时检测本地域控信息，防止个人与办公设备混用。

2.数据防泄漏管控策略

梳理企业内部敏感关键词，通过防泄漏能力创建保密规则，阻断或审计内部商密信息通过第三方IM、网盘、协议、介质拷贝（外发）等媒介向外传输泄密。

内部IM软件在移动端应集成前序提及的OA、邮箱、云盘等办公模块，且支持文档在线协同不落地原则。

05

总结

总结与思考

通过深度解读国家三法一条例
制定内部管理制度
合规审计梳理自查风险
加强数据全生命周期保护措施

数据安全建设还有哪些可以闭环

THANKS

感谢您的观看