[公开]360NELab-DST-0-060-20210927

大数据协同安全技术
国家工程实验室
National Engineering Laboratory for Big Data Collaborative Security Technology

全球数据安全观察

总第 60 期 2021 年第 36 期

（2021.09.13-2021.09.26）

大数据协同安全技术国家工程实验室

目录

政策形势

1、天津市：开展数据共享开放评价 促进数据资源高效利用

近日，天津市委网信办、天津市大数据管理中心联合印发《天津市数据共享开放评价实施方案》，综合考虑各要素作用于数据共享开放所产生的效应，进行重点、全量、多维度的评价，客观、细化、量化地评价政务数据共享和公共数据开放的规模、成效、能力和水平，进一步规范和促进天津市政务信息资源共享和公共数据资源开放。

https://mp.weixin.qq.com/s/EZZ40KUo4_2IoNdI4-8agA

2、工信部：加强车联网网络安全和数据安全工作

9 月 16 日，据工业和信息化部网站消息，工业和信息化部发布《关于加强车联网网络安全和数据安全的通知》。

通知指出，要加强智能互联车辆的安全防护，加强车联网安全防护，加强车联网服务平台的安全防护，加强数据安全防护，完善安全标准体系。在加强车联网网络安全防护方面，各相关企业应建立网络安全监测预警机制和技术手段，对智能车联网进行网络安全相关监测，车辆互联网服务平台和联网系统，及时发现网络安全事件或异常行为，并按规定保存相关网络日志不少于 6 个月。

https://mp.weixin.qq.com/s/WP4NMi4ya_eLdyQ71roeMg

3、六部门强化教育 App 网络与数据安全监管，涉及等保、数据本地化、评估等多项要求

近日，教育部办公厅等六部门发布《关于做好现有线上学科类培训机构由备案改为审批工作的通知》，其中要求线上机构具备自有或租用的性能可靠的服务器，且服务器必须设置在中国内地。教育移动应用提供者应当建立覆盖个人信息收集、储存、传输、使用等环节的数据保障机制，储存 100 万人以上个人信息的线上校外培训 APP，应通过个人信息保护影响评估、认证或合规审计。

http://www.moe.gov.cn/jyb_xwfb/gzdt_gzdt/s5987/202109/t20210918_564444.html

4、国家标准《重要数据识别指南（征求意见稿）》发布

2021 年 9 月 23 日，《信息安全技术 重要数据识别指南》征求意见稿完成，该标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口，主要起草单位为中电数据服务有限公司 、中国电子技术标准化研究院 、中国信息安全测评中心等。

数据识别指南征求意见稿明确了识别重要数据的基本原则，提出了重要数据的特征，主要包括**与经济运行相关、与人口与健康相关、与自然资源与环境相关、与科学技术相**

关、与安全保护相关、与应用服务相关、与政务活动相关等类别。

https://mp.weixin.qq.com/s/gFzplMy-EPVa5AjsKSu3Ew

5、巴西政府发布数据保护指南

据报道，巴西政府近期推出了数据保护指南，以提高公众意识。该指南由政府与国家数据保护机构合作编写，详细说明了数据用户的权利，包括选择退出的权利、如何保护个人信息以及如果他们遭遇数据泄露应采取哪些措施。该报告还概述了组织针对个人数据应采取行动的步骤。

https://iapp.org/news/a/brazil-launches-data-protection-guide/

业界观点

1、周鸿祎：以安全新体系筑牢数字安全屏障

9 月 26 日，2021 世界互联网大会乌镇峰会正式开幕，三六零集团创始人、董事长周鸿祎出席开幕式并发表主题演讲。

周鸿祎在论坛上介绍，数字文明新时代有着“一切皆可编程、万物均要互联、大数据驱动业务”的特征，其本质是软件重新定义整个世界。要构建和守护网络空间命运共同体，解决数字化复杂安全问题，必须要有体系化的解决方案。但传统安全作为信息化的附庸，缺乏顶层设计，依靠单个产品或多个产品不断堆砌，无法形成体系化的解决方案。因此要用数字化思维重塑网络安全，构建新战法、新框架和新能力，形成面向数字化的安全新体系。

360 构建了新一代安全能力框架，即 360 安全大脑能力框架。它作为数字化安全体系的一个整体结构，涵盖攻击面防御、资源面管控、数据运营、专家运营等 4 大类共 20 个基础设施，可支撑云安全、大数据安全等基础安全体系建设和工业互联网、车联网、智慧城市等行业安全场景。

https://mp.weixin.qq.com/s/z0s8ijJL4iejs5d7kdImRw

2、人民网：金融科技应用要加强对数据隐私与安全的保护

中国银保监会统计与信息监测部副主任骆絮飞表示要坚持数据驱动，发挥数据要素倍增作用；要坚持开放连接，银行业、保险业要与政府、社会、个人等社会经济主体建立广泛的数字连接，形成以数据循环流动为基础，多主体数字化协同生态体系；要坚守风险底线，加强战略风险、价值链风险、算法模型风险的管控，提高网络安全保障能力，防范攻击威胁，提升数据安全的防护水平。

http://finance.people.com.cn/n1/2021/0920/c1004-32232007.html

3、从《数据安全法》到“重要数据”的思考

2021 年 9 月 1 日，《中华人民共和国数据安全法》（以下简称《数据安全法》）正式施行，数据安全保护被国家提升到了重要高度。关于“重要数据”的几点思考：**1.重要数据是非涉密数据。**通过调研与分析，可得重要数据是非涉密数据。因此，重要数据首先排除是国家秘密。**2.重要数据是属于数据分级范畴。**重要数据这个概念因为数据分类分级保护制度而来，重要数据应该是“数据分级”的一个重要概念，而不把它归在“数据分类”范畴。**3.重要数据目录制定要从各部门各行业着手。**《数据安全法》提出重要数据目录要国家

数据安全工作协调机制统筹协调有关部门制定。而数据本身具有和业务强耦合的特点，因此数据分类分级和重要数据目录必然要从具体部门和行业从下而上细化。**4.关键信息基础设施运营的重要数据是重要数据的一方面。**

https://www.secrss.com/articles/34573

4、CNCERT：汽车数据出境态势分析报告

CNCERT 依托宏观数据，联合智联出行研究院（ICMA）对 15 类主流车型近期的数据出境情况进行分析，结果如下。**1.车辆识别码等汽车数据大量出境。**类似于身份证号是中国公民的唯一标识，车辆识别码是汽车的唯一标识。共发现我国境内车辆识别码通过网络出境超过 100 万次，单日最大出境规模近 8.3 万次。**2.汽车数据出境场景复杂多样。**发现存在汽车数据出境行为的境内 IP 地址 45,638 个，覆盖境内全部 31 个省级行政区。**3.汽车数据出境行为普遍存在。**整体来看，汽车数据出境并只不是某类汽车品牌的个别行为，而是涉及多类汽车品牌的普遍行为。**4.出境数据涉及个人信息和重要数据。**分析发现，部分出境数据涉及了身份证号（行驶证号）、驾驶证档案编号、车牌号、手机号等。

https://www.secrss.com/articles/34468

5、46%的本地数据库系统存在安全漏洞

根据 Imperva 一项为期五年的新研究，全球 46%的本地数据库包含安全漏洞，其中大多数是严重或者高危漏洞。Imperva 在五年内扫描了全球 2.7 万个数据库，发现平均每个数据库包含 26 个漏洞，其中约 56%都是严重或者高危漏洞。这意味着一旦被利用，会导致严重的危害。

报告指出，很多国家的数据库都存在超过全球平均水平的漏洞，无论是在易受攻击的数据库百分比方面，还是在每个数据库的平均漏洞数量方面都是如此。即使是德国这样的脆弱数据库比例相对较低（19%）的国家，漏洞的平均数量仍然相对较高，需要改进。同时，虽然基于云的平台越来越受欢迎，但大多数组织继续将最敏感的数据存储在本地。而这些本地数据库中普遍存在一些多年未得到解决的 CVE 漏洞。

https://mp.weixin.qq.com/s/8mG8EmKsSEg71Mqdav9SZQ

安全事件

1、38 亿条涉及 Clubhouse 和 Facebook 用户记录的数据库正在暗网出售

2021 年 9 月 24 日，据外媒报道，一个流行的黑客论坛上的用户正在出售一个据称包含 38 亿条用户记录的巨量数据库。据称，该数据库是通过将之前抓取的 Clubhouse “秘密数据库”中的 38 亿个电话号码与用户的 Facebook 个人资料结合起来编制的。这些记录包括姓名、电话号码、Clubhouse 排名和 Facebook 个人资料链接。

https://securityaffairs.co/wordpress/122532/cyber-crime/clubhouse-facebook-data-scraping.html?web_view=true

2、1.06 亿条泰国游客的个人数据发生泄露

2021 年 9 月 21 日，据报道，安全研究人员发现网上暴露了一个不安全的数据库，其中包含了数百万泰国游客的个人信息。该专家于 2021 年 8 月 22 日发现了不安全的数据库，并立即通知了泰国当局，他注意到存档中存储的一些数据可以追溯到十年前。虽然数据库的 IP 地址仍然是公开的，但数据库已脱机并已被蜜罐取代。该数据库大小为 200GB，包含多项资产，包括超过 1.06 亿条记录。暴露的记录包括全名、抵达日期、性别、居留身份、护照号码、签证

信息和泰国入境卡号码。

https://securityaffairs.co/wordpress/122418/data-breach/thailand-visitors-leaked-online.html

3、Black Matter 勒索团伙向农村合作社索要 590 万美元赎金

2021 年 9 月 21 日， BlackMatter 勒索软件团伙袭击了美国农民合作社 NEW Cooperative，并要求支付 590 万美元的赎金。勒索软件团伙声称窃取了 1000 GB 数据，包括 soilmap.com 项目的源代码、财务信息、网络信息、研发结果、敏感员工信息、法律和执行信息以及 KeePass 导出。如果在五天内没有支付赎金，勒索软件运营商威胁要加倍赎金。

https://securityaffairs.co/wordpress/122410/cyber-crime/black-matter-new-cooperative.html

4、全球第三大班轮公司法国达飞轮船遭网络攻击，客户信息遭泄露

2021 年 9 月 20 日，全球第三大班轮公司法国达飞轮船在官网公布遭遇网络袭击，部分客户信息泄露，达飞称 IT 团队已更新安全补丁。事实上，除达飞轮船外，包括马士基、MSC、中远海运等多家大型集运公司都曾遭遇过网络袭击。

https://baijiahao.baidu.com/s?id=1711563665845568560&wfr=spider&for=pc

5、南非司法部遭勒索软件攻击，导致无法使用所有电子服务

2021 年 9 月 17 日，据外媒报道，南非司法和宪法发展部正在努力恢复其运作，因为最近的勒索软件攻击加密了其所有系统，导致内部和公众无法使用所有电子服务。作为攻击的后果，司法和宪法发展部表示，儿童抚养费的支付现在被搁置，直到系统重新上线。

https://www.cnbeta.com/articles/tech/1180077.htm