[公开]360NELab-DST-0-023-20201221

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 23 期 2020 年第 23 期

（2020.12.14-2020.12.20）

大数据协同安全技术国家工程实验室

摘要

本期全球数据安全观察搜集到的重要实践的主要类型为**数据泄露**、**勒索软件**以及**数据合规**问题。

1. 上海 190 万中国共产党员详细信息泄露
2. 美国百万名牙科患者数据泄露
3. 全球 4500 万医学影像照片在线暴露
4. 加州医院 67000 名患者数据被泄露
5. UiPath 数据被泄露
6. FireEye、美国财政部和商务部被 APT 29 攻击，18000 名客户面临“窃听”威胁
7. 英特尔旗下 AI 处理器实验室遭勒索攻击
8. Twitter 因违反数据保护条例被欧盟罚款 55 万美元
9. 大多数企业都在客户不知道的情况下收集数据
10. 苹果新规：开发者须明确提供收集的用户隐私信息

此外在数据安全技术与观点方面主要讨论了：

欧盟《数字服务法》草案；《信息安全技术 政务信息共享 数据安全技术要求》标准；2021 数据加密趋势；数字化时代个人金融信息的保护；APP 的个人信息保护；信通院发布《全球数字治理白皮书（2020）》以及数据跨境流动的制度与技术建设。

全球动态

1、上海 190 万中国共产党员的详细信息泄露

2020 年 12 月 14 日，KELA 的研究人员分析了一个最近在网上泄漏的数据库，该数据库包含有关上海 190 万中国共产党员的数据，包括成员的姓名、性别、种族、家乡、组织、身份证号码、地址、手机号码、座机和教育程度。

https://securityaffairs.co/wordpress/112382/data-breach/chinese-communist-party-db-leak.html

2、美国百万名牙科患者数据被泄露

2020 年 12 月 17 日，美国一家医疗服务提供商开始通知 100 多万名患者，他们的数据可能因网络攻击而被泄露。在此次安全事件中可能访问的患者数据包括姓名、地址、牙科诊断和治疗信息、患者账户号码、账单信息、银行账户号码、患者牙医的姓名和医疗保险信息。

https://www.csbit.cn/article/63/1350.html

3、全球 4500 万医学影像照片在线暴露

2020 年 12 月 16 日报道，近日，根据 CybelAngel 最新发布的为期六个月的调查报告，由于存储、发送和接收医疗

数据的技术存在安全问题，全球已经发现超过 4500 万张医学图像以及与之相关的个人身份信息（PII）和个人医疗保健信息（PHI）在线暴露，，这些图像被存储在 67 个国家（包括美国、英国、法国和德国）的 2140 台未受保护的（NAS）服务器上。

https://www.secrss.com/articles/27932

4、加州医院 67,000 名患者数据泄露

2020 年 12 月 15 日，据外媒报道，加利福尼亚州的一家医院已经通知 67,000 名患者，他们的个人数据可能已受到网络攻击，患者的姓名，地址，出生日期，保险公司号码可能已经暴露。该医院表示，目前尚不清楚任何滥用或企图滥用患者健康信息的情况。

https://www.infosecurity-magazine.com/news/svh-notifies-67k-patients-of-data/

5、UiPath 披露数据泄露

UiPath 是一家生产机器人自动化软件的初创公司，目前因遭受网络攻击而导致信息泄露。该文件包含诸如实名、电子邮件地址、用户名、公司名称、国家/地区的详细信息，以及注册了公司在线学习平台 UiPath Academy 的用户的

UiPath 认证详细信息 。

https://securityaffairs.co/wordpress/112267/data-breach/uipath-data-leak.html

6、FireEye、美国财政部和商务部被 APT 29 攻击，18000 名客户面临“窃听”威胁

黑客利用 SolarWinds 在今年 3 月至 6 月间发布的的网络管理产品 Orion 更新，植入恶意代码，从而入侵了美国财政部、商务部下属的国家电信和信息管理局(NTIA)、FireEye 的网络。

https://www.freebuf.com/news/257878.html

7、英特尔旗下 AI 处理器实验室遭勒索攻击，数据被盗

2020 年 12 月 15 日，英特尔(intel)旗下的人工智能芯片制造商哈瓦那实验室(Habana Labs)遭到 Pay2key 勒索软件运营商的攻击，该运营商声称他们已经侵入了英特尔旗下的 Habana 实验室网络，并窃取了 53GB 数据，包括有关名为 Gaudi 的新人工智能芯片代码的信息。

https://www.secrss.com/articles/27893

8、 Twitter 因违反数据保护条例被欧盟罚款 55 万美元

2020 年 12 月 15 日，爱尔兰数据保护委员会（DPC）对 Twitter 处以 45 万欧元（约合 54.7 万美元）的罚款，原因是 Twitter 未能按照欧洲数据隐私法规《通用数据保护条例》（GDPR）的规定，及时公布并妥善记录一起数据泄露事件。

https://mp.weixin.qq.com/s/5U0bA73__hdLvnmUBeaAXg

9、调查：大多数企业都在客户不知道的情况下收集数据

2020 年 12 月 16 日，据外媒报道，总部位于德克萨斯州奥斯汀的企业 Zoho 于 2020 年 11 月对美国和加拿大的 1,416 个人进行了调查。研究结果表明，在消费者不知道情况下，不道德的数据收集策略常被用来捕获信息，尤其在 B2B 领域。

https://www.zdnet.com/article/most-businesses-are-tracking-customers-yet-dont-tell-them/

10、苹果新规：开发者必须提供明确的收集用户隐私信息

2020 年 12 月 16 日报道，近日，苹果开始在 iOS、iPadOS、macOS、watchOS 和 tvOS 的所有应用商店中发布隐私摘要，开发者需要告知苹果应用程序是否收集了姓名、电子邮件地址、电话号码、家庭住址以及健康和健身数据等信息。

https://mp.weixin.qq.com/s/BP1CwOAUuzSsM53BEpoM4w

业界观点

1、欧盟《数字服务法》草案：重点监管科技巨头，最高罚款达全球营收的 6%

据 Politico 报道，欧盟《数字服务法》草案显示，**大科技公司可能会面临与在线活动相关的巨额罚款，尤其是定向广告。根据该草案，违规公司可能会面临最高达到年收入 6%的罚款。**《数字服务法》还将授权“数字服务协调员”监管大科技公司的合规情况，包括用于定向或精准广告的算法是否合法。欧盟委员会的计划是更严格地监管 Facebook 和亚马逊等公司，以及**监管平台如何规制网上非法内容。**

https://www.secrss.com/articles/27844

2、《信息安全技术 政务信息共享 数据安全技术要求》标准解读

该标准通过充分调研和梳理政务信息共享的数据流程，抽取共性，分析政务信息数据流转的过程及面临的数据安全风险，梳理安全控制点等，总结现有各种数据安全技术应对政务信息共享过程中面临数据风险的能力，提出政务信息共享数据安全技术要求框架，规定了政务信息共享过程中共享数据准备、共享数据交换、共享数据使用阶段的数据安全技

术要求以及相关基础设施的安全技术要求。

https://mp.weixin.qq.com/s/GxxK5mNp32vcOJRSLTBeDg

3、2021 年数据加密的六大趋势

2021 年，加密技术有望迎来重大变革，以下为 2021 年值得关注的六大加密趋势：(1) 云计算将扮演更重要的角色，尤其是在金融服务领域；(2) 同态加密将成为“新常态”；(3) 自带加密（BYOE）将开始流行；(4) 加密+密钥管理，对于缩短的证书生命周期至关重要；(5) 加密技术对 DevSecOps 很重要，尤其是代码签名；(6) 长周期设备制造商将开始拥抱加密敏捷性。

https://www.aqniu.com/industry/71625.html

4、数字化时代个人金融信息保护的思考

数字化时代下加强个人金融信息保护需要政府、市场、社会等多方面协同：**一是**持续完善制度规范，适应经济金融数字化转型的实际情况；**二是**增强监管科技能力，进一步完善个人金融信息保护的监管分工和统筹机制;**三是**发挥行业自律作用，各行业协会要相互沟通，形成合力；**四是**提升机构的履责水平，完善内部监督和责任追究机制；**五是**加强社会公众参与度，充分调动社会公众参与个人信息安全的治理。

https://mp.weixin.qq.com/s/WtKdNZAJRCTdgYKDE7vfaQ

5、聚焦个人信息保护：App 手别伸得太长了

当前，我国 App 在架数量已经超过 350 万款,成为千行百业的移动互联网入口，极大地方便了人民群众的工作生活。但与此同时，App 侵害用户权益的事件时有发生，广大用户反应强烈，部分 App 多次整改后问题依然突出。强化个人信息保护，必须标准先行。只有标准化，才能实现监管检测的自动化、智能化。

https://finance.sina.com.cn/tech/2020-12-16/doc-iiznezxs7222486.shtml

6、中国信通院发布《全球数字治理白皮书（2020 年）》

2020 年 12 月 15 日，中国信通院发布了《全球数字治理白皮书（2020 年）》。这是继 2017 年以来，中国信通院连续第四年发布数字治理相关白皮书，内容包括全球数字治理的多边框架、双边和区域性机制、私营部门治理，以及全球数字治理展望等内容。

https://mp.weixin.qq.com/s/DpIKktwa8J7_x76wBiPdlQ

7、数据跨境流动的制度建设与技术支撑

从全球范围看，数据流动对全球经济增长的贡献已经超过传统的国际贸易和投资。各国高度关切数据跨境流动。美国凭借其产业国际竞争优势和强大灵活的保障能力，以长臂管辖抢夺他国“治外法权”。欧盟对数据出境进行严格限制，其主要原因是担心接收国家或企业降低个人数据保护标准，因而采取了以充分性认定机制为主的国际制度协同框架，旨在优先保护个人信息安全。新兴经济体的数据战略则以防守型为主，更多地强调数据本地化存储，意图“划疆而治”。

一般而言，当一国的公共部门或私人部门想要传输数据给接收国的公共部门或私人部门，即使是数据主体方与接收方之间已经达成规制性协定，在大多数情况下也需要分别向本国与对方国的主管部门提交申请，在获得批准之后方可执行数据跨境流动。

除了制度建设，各类信息创新技术也是支持数据跨境合规有序、高质量流动的有效工具。按照《信息安全技术-数据出境安全评估指南（征求意见稿)》的要求，重要数据在出境前，应对其采取脱敏等技术处理措施，并对脱敏处理的效果进行验证，以达到合理程度的不可还原。下面以支付标记化技术、区块链技术、联邦学习等为例，谈谈如何依靠技术手段实现数据隐私保护和数据应用之间的平衡。