[公开]360NELab-DST-0-035-20210322

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 35 期 2021 年第 11 期

（2020.03.15-2021.03.21）

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事件的主要类型为**数据丢失泄露、勒索软件**和**数据安全合规问题**。

1. 美国运输管理软件公司的敏感数据在线暴露
2. 日本最大社交应用未经用户同意访问用户数据
3. Descartes Aljex 配置错误泄露 103GB 数据
4. 黑客从已失效的违规网站泄漏了付款数据
5. 宏碁遭勒索软件攻击，5000 万赎金创世界纪录
6. 美国国会再次提出联邦隐私法案
7. 沃达丰西班牙分公司违反 GDPR 被罚款近千万美元
8. 央视 315 晚会集中曝光侵犯个人信息行为

此外，在数据安全技术与观点方面主要讨论了：

1. 可信执行环境浅析及应用实践
2. 商业银行数字化转型的数据治理问题
3. 加紧制定《数据安全法》《个人信息保护法》
4. 揭开数据本地化的面纱：数字贸易中的大国博弈
5. 个人信息与数据保护相关内容摘录
6. 隐私计算领域发展的三个方向
7. 确保数据安全的关键在哪里？
8. 2021 年数据报告

全球动态

1. 美国运输管理软件公司的敏感数据在线暴露

3 月 16 日，据外媒报道，一家美国运输管理软件公司的 103 GB 的数据价值暴露在配置错误的云服务器上。本次事件影响了 4,000 多人，公开的数据包括货件信息、收货人姓名、货件起运地和目的地、地址和电话号码等。

https://www.hackread.com/shipping-management-software-firm-data-online/?web_view=true

2. 日本最大社交应用 LINE 主动报告数据违法行为：未经用户同意允许境外第三方访问用户数据

3 月 17 日报道，日本“连我”（LINE）用户的个人信息曾处于中国相关公司技术人员可以阅览的状态。LINE 公司向用户提示的数据管理方法相关指引中并未就来自海外的访问进行充分说明。LINE 以应对措施存在问题为由，向日本政府个人信息保护委员会报告。近期将设置由外部专家组成的第三方委员会展开调查。

https://mp.weixin.qq.com/s/pxJt-BNHUqYLffGpyEJWcA

3. Descartes Aljex 因 AWS S3 配置错误泄露 103GB 数据

2021 年 3 月 16 日，Website Planet 发现运输管理软件 Descartes Aljex 因 AWS S3 存储桶配置错误泄露了 103 GB 数据。此次事件影响了该公司的客户、员工、销售代表以及为第三方员工，泄露了姓名、电话号码，电子邮件地址，Aljex 用户名和纯文本密码等个人信息，和收件人姓名、货件起运地和目的地、地址和电话号码等货件信息。

https://www.hackread.com/shipping-management-software-firm-data-online/

4. 黑客从已失效的 WeLeakInfo 违规网站泄漏了付款数据

2021 年 3 月 16 日，WeLeakInfo.com 是一个数据泄露通知服务，它允许其客户验证其凭据是否在数据泄露中受到破坏。该网站声称发生数据泄露事件，网络安全情报公司 Cyble 与 BleepingComputer 分享了被盗数据的样本，并说大约有 10000 个唯一客户列在数据泄漏中。泄漏的数据包括 Stripe WeLeakInfo 帐户的屏幕截图以及包含发票、成功付款、客户列表等的电子表格。

https://www.bleepingcomputer.com/news/security/hacker-leaks-payment-data-from-defunct-weleakinfo-breach-site/

5. 宏碁遭勒索软件攻击，5000 万赎金创世界纪录

3 月 20 日，计算机巨头宏碁（Acer）受到勒索软件 REvil 攻击，勒索赎金高达五千万美元，创下勒索软件赎金的新记录。泄漏数据的截图包括财务电子表格、银行对账单等文档。

https://mp.weixin.qq.com/s/roqi1kSMdcnHCHuaNNea-Q

6. 美国国会再次提出联邦隐私法案

3 月 15 日消息，美国众议员 Suzan DelBene 重新提出了一项法案，该法案将创建一个全国范围的数据隐私标准。若该法案通过，将取代各州制定的隐私法案。

https://www.bleepingcomputer.com/news/software/wordpress-plans-to-drop-support-for-internet-explorer-11/

7. 沃达丰西班牙分公司违反 GDPR 被罚款近千万美元

2021 年 3 月 16 日，电信公司沃达丰西班牙分公司因违反 GDPR 被罚款近千万美元。该公司因使用不适当的电话销售策略以及未能保护数据而导致了 4 项罚款，共计 972 万美元。 前两项罚款与《通用数据保护条例》（GDPR）有关，总计 716 万美元。第三项罚款与西班牙数字版权和电信的法律以及 GDPR 有关，为 239 万美元。第四项罚款涉及西班牙 Cookie 的法律，为 17.9 万美元。

https://www.infosecurity-magazine.com/news/aepd-issues-highest-ever-fine/

8. 央视 315 晚会集中曝光侵犯个人信息行为，涉及人脸识别滥用、隐私泄露等问题

2021 年 315 晚会上，科勒卫浴多个门店均装有人脸识别摄像头捕捉进店顾客人脸信息，提供这类人脸识别技术的涉事企业包括万店掌、悠络客、雅量科技、瑞为。前程无忧、猎聘等招聘平台大量简历流向黑市，老人手机里的“清理大师”APP 打着安全提示的旗号，蒙骗老人，在消费者不知情的情况下随意收集、任意滥用。

https://mp.weixin.qq.com/s/RjAYYwnukfwheoLU_8xWwA

业界观点

1. 可信执行环境浅析及应用实践

可信执行环境技术凭借其芯片级的保护方案，具有高安全性、高性能、高通用性等优势，在数据联合金融风控、交易隐私保护、区块链、人工智能、医疗等领域有着广阔的应用前景。本文浅析可信执行环境的技术原理、发展历程和应用场景，并介绍基于可信执行环境的可信计算应用实践。

https://mp.weixin.qq.com/s/qC6O8etDTn6vb3Ajsarifw

2. 商业银行数字化转型的数据治理问题

近年来，数字经济蓬勃发展推动了商业银行的数字化转型。突如其来的新冠疫情，给商业银行带来不同程度的影响，也成为商业银行数字化转型的助推器和催化剂。随着数字化转型步伐的加快，对数据治理提出了更高要求，商业银行数据质量、数据标准和数据安全问题面临的困境变得尤为突出。商业银行应当采取措施妥善应对，切实做好数据治理工作，提高数据治理水平，完善数据治理架构，提高数据质量，建立健全数据标准体系，切实保障数据安全，在业务经营、风险防控、内部管理与监管合规等方面充分发挥数据的作用，利用数据治理，实现数据驱动决策，为高质量发展夯实

数据基础。

https://mp.weixin.qq.com/s/78RArzhoy5BwfJ6_MT0r4g

3. 国家网信办副主任：加紧制定《数据安全法》《个人信息保护法》

从全国两会到央视“315”晚会，数据隐私安全问题被不断提起。随着数字经济时代的到来，数据成为一种新型的生产要素和社会财富被不断分享、分析、利用，随之而来的个人隐私安全问题也成为数字社会首要关注点。

2021 年 3 月 19 日，国新办就第四届数字中国建设峰会有关情况举行发布会，针对大数据环境下个人隐私安全的保护，国家互联网信息办公室副主任杨小伟介绍，《数据安全法》《个人信息保护法》正在加紧制定出台。

https://mp.weixin.qq.com/s/fd5W1TNeRUuLBmM70WQ0qg

4. 揭开数据本地化的面纱：数字贸易中的大国博弈

当前全球数字经济高速发展，大国围绕“数据本地化”展开博弈，对“数字本地化”政策大致形成了“美国反对、中国与欧盟中立、俄罗斯与印度提倡”三种不同态度。眼下，而各国对“新型石油资源”的争夺战，预示着全球数字地缘版图内的大国博弈还将继续。

https://www.secrss.com/articles/29983

5. “十四五”规划纲要：个人信息与数据保护相关内容摘录

《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》共分为19篇，其中与个人信息、数据保护以及网络安全密切相关的内容集中于第五篇“加快数字化发展 建设数字中国”；同时，第三篇“加快发展现代产业体系 巩固壮大实体经济根基”、第六篇“全面深化改革 构建高水平社会主义市场经济体制”、第十一篇“推动绿色发展 促进人与自然和谐共生”部分章节也与数据安全密切相关。

https://mp.weixin.qq.com/s/qOk5_-tAXDK3M3g2njdK5Q

6. 隐私计算领域发展的三个方向

2020年被公认为隐私计算元年，其重要标志就是隐私计算正式从理论走向实践，从开发走向应用，其中以金融及医疗行业应用为典型代表。隐私计算计算领域的发展可以分为三个方向：**MPC/同态加密，联邦学习以及TEE/沙箱。**

MPC/同态加密也称为多方安全计算和同态加密，实现方法完全不同，但是信任假设是相同的。假如没有任何可以信任的第三方，便可以采用联邦学习。联邦学习是解决模型训

练、模型推断的问题，在机器学习方面来解决没有信任的前提下，如何做联合模型训练和推断。但这个方式的缺陷在于计算的方式仅仅是在机器学习的方式。如果有可以信任的第三方，就可以采用安全计算的方式计算出结果。在这里，安全计算中主要防备的是应用本身对平台产生的威胁。安全沙箱做得好，对系统本身产生的风险小，就可以安全将它算出来。但与此同时，第三方中间需要有特殊的硬件——TEE，Trusted Execution Environment，也叫可信任执行环境。

https://mp.weixin.qq.com/s/CkAmHDgIAjoKDX-9kuI8bA

7. 确保数据安全的关键在哪里？

随着信息网络的高速发展，非法获取公民个人信息并出售的行为屡屡发生，严重危害了公民个人信息安全，正是因为如此，数据安全成为了两会热点话题。2021 年 3 月 3 日的全国政协十三届四次会议新闻发布会的消息显示，《个人信息保护法》草案已经提请全国人大常委会审议，这一法律的颁布和实施，对保护个人信息安全将发挥重要的作用。除此之外，全国人大代表和政协委员围绕“数据安全”提出加强公民信息保护，加快数据产权立法等建议。

https://mp.weixin.qq.com/s/60BPDqCjysUYHHhpl3paPw

8. 2021 年数据报告

IAB 发布“2021 年数据报告”，评估第三方 Cookie 和标识符跟踪生态系统的感知准备与实际准备情况。一是行业的强烈备灾意识与其担忧和挑战形成鲜明对比，二是继续过度依赖第三方数据，三是行业需要更积极地规划后第三方 Cookie/ID 生态系统的潜在财务影响，四是行业合作、隐私优先寻址解决方案和第一方数据是成功的关键。

https://mp.weixin.qq.com/s/cfMX61dRimJQIqaphj3ilw