[公开]360NELab-DST-0-029-20210201

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 29 期 2021 年第 5 期

（2020.01.25-2021.01.31）

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**数据泄露、泄露数据买卖**和**勒索软件问题**。

1. 几乎所有巴西人的个人信息均被泄露
2. 印度加密交易所遭攻击，超 32.5 万用户数据泄露
3. TikTok 漏洞可能暴露用户个人资料和电话号码
4. 228 万约会网站用户数据被泄露
5. 包含 1.76 亿巴基斯坦手机用户的数据库被在线销售
6. 美国军方正在从普通应用程序中购买位置数据
7. 零售巨头牛奶集团遭勒索攻击，赎金 3000 万美元
8. 英国研究与创新机构遭遇勒索软件攻击

此外，在数据安全技术与观点方面主要讨论了：

1. 2020 年勒索软件利润暴涨 311%
2. 加大 APP 整治力度，维护个人信息安全、数据安全
3. 自由与安全：数据跨境流动的中国方案
4. 数据安全范式革新及其立法展开
5. 2020-2021 年度数字经济形势分析
6. 安全基线建设指南
7. 同态加密：密码学的下一个黄金时代

全球动态

1. 巴西一数据库发生重大数据泄露事件: 几乎巴西所有人信息均被泄露

2021 年 1 月 26 日报道，泄露的数据为 14 GB，包含了 1.04 亿车辆和 4000 万家企业详细信息，潜在受影响人数 2.2 亿。巴西人口 2.1 亿，这意味着巴西所有人的信息都被泄露（还有部分在巴西生活的外籍居民）。泄露的信息包含了姓名、出生日期和 CPF 号码。CPF 号码是巴西税务局分配给居民和需要纳税的外籍居民的数字。网络安全公司对钓鱼骗局发出了警告。

https://www.cnbeta.com/articles/tech/1082831.htm

2. 印度加密交易所 BuyUCoin 遭攻击，超 32.5 万用户个人数据泄露

2021 年 1 月 25 日，一个名为 ShinyHunters 的黑客组织泄露了一个数据库，其中包含超过 32.5 万 BuyUCoin 用户的姓名、电话号码、电子邮件地址、税务身份号码和银行账户详细信息。

https://www.cnbeta.com/articles/tech/1082319.htm

3. TikTok 漏洞可能暴露用户的个人资料数据和电话号码

2021 年 1 月 26 日，据外媒报道，网络安全研究人员披露了 TikTok 中现已修复的安全漏洞，该漏洞可能使攻击者能够建立该应用程序的用户及其关联电话号码的数据库，用于将来的恶意活动。

https://thehackernews.com/2021/01/tiktok-bug-could-have-exposed-users.html

4. 黑客泄露了 228 万约会网站用户数据

2021 年 1 月 25 日报道，一名黑客在黑客论坛公开了 228 万约会网站 MeetMindful.com 注册的用户数据，可以免费下载。泄露数据容量约 1.2 GB，包含了部分敏感的用户真实信息，包括真实姓名、地址和邮编、电子邮件、约会偏好、婚姻状况、出生日期、经纬度、IP 地址、Bcrypt 哈希的账号密码、Facebook 用户 ID、Facebook 身份验证令牌等。

https://finance.sina.com.cn/tech/2021-01-25/doc-ikftpnny1380924.shtml

5. 包含 1.76 亿巴基斯坦手机用户的数据库被在线销售

2021 年 1 月 27 日，黑客正在出售一个据称包含超过 1.76 亿巴基斯坦公民个人详细信息的数据库。显然，该数据库是

该国不同电信公司的数据的汇总，并全部被出售以获取利润。该数据库包含的个人数据中包括全名，实际地址和电话号码。

https://www.hackread.com/pakistani-mobile-phone-users-database-sold-online/

6. 美国军方正在从普通应用程序中购买位置数据

2021 年 1 月 29 日报道，一款下载量超过 9800 万次的穆斯林祈祷应用程序，与一个广泛的供应链相连，将普通人的个人数据发送给经纪人、承包商和军方。美国军方正在购买从大众应用程序中收集的世界各地人员的精细动态数据。根据分析报道，在此类程序中，最受欢迎的应用是穆斯林祈祷和古兰经应用，在全球范围内下载量超过 9800 万，其他包括穆斯林约会应用程序还有流行的 Craigslist 应用程序。

https://mp.weixin.qq.com/s?__biz=MzA3Mjc1MTkwOA==&mid=2650475891&idx=1&sn=3a003da3e532a8a536f370a506afed9c

7. 零售巨头牛奶集团遭勒索攻击，赎金高达 3000 万美元

2021 年 1 月 26 日，泛亚大型零售连锁运营商 Dairy Farm Group 本月受到 REvil 勒索软件攻击。攻击者声称要求 3000

万美元的赎金。乳业集团在亚洲拥有 10000 多个网点，并拥有 230000 名员工。

https://www.bleepingcomputer.com/news/security/pan-asian-retail-giant-dairy-farm-suffers-revil-ransomware-attack/

8. 英国研究与创新机构遭遇勒索软件攻击

2021 年 1 月 30 日，据外媒报道，英国研究与创新（UKRI）机构披露遭遇勒索软件攻击。UKRI 成立于 2018 年 4 月，是由英国商业、能源和工业战略部(BEIS)赞助的非部门公共机构。攻击导致两项服务受到影响，一项是 UKRI 位于布鲁塞尔的英国研究办公室（UKRO）的门户网站，另一项是 UKRI 各理事会使用的外联网。尚不清楚攻击者是否从英国机构窃取了数据。

https://securityaffairs.co/wordpress/114026/hacking/ukri-ransomware-attack.html

业界观点

1. 2020 年勒索软件利润暴涨 311%

与暗网市场有关的犯罪从 2019 年到 2020 年有所增加，勒索软件的利润激增。Chainalysis 报告称，勒索软件占犯罪获得资金总额的 7%，价值近 3.5 亿美元的加密货币，这个数字比 2019 年增长了 311%。在 2020 年，没有其他类别的基于加密货币的犯罪上升如此之快。专家称，可能是员工大规模转移到远程工作导致的这项结果，犯罪分子试图利用 COVID-19 大流行来利用企业基础架构中的潜在漏洞。

https://www.bankinfosecurity.com/good-news-cryptocurrency-enabled-crime-took-dive-in-2020-a-15820

2. 工信部：加大 APP 整治力度，维护用户个人信息安全、数据安全

随着信息化发展，个人信息保护更加重要。为了更好地保护用户权益，工信部采取了一系列措施，尤其是采取了专项整治，取得了积极的成效。去年主要采取了四项举措：**一是开展专项治理；二是推动标准制定；三是强化手段的建设；四是加强行业自律**。下一步在这个基础上，工信部会进一步

加大力度。总的来看，一定要维护用户个人的信息安全、数据安全，使消费环境实现根本性好转。

https://mp.weixin.qq.com/s/KEuNvCDLh6CQwc6Bu8IGxw

3. 自由与安全：数据跨境流动的中国方案

各国近年来就数据跨境是否以自由流动为原则、数据跨境管制是否具有正当性等议题存在重大分歧。我国《数据安全法（草案）》首次提出“数据安全自由流动原则”，将“数据自由流动”作为基础性原则，将“数据安全流动”作为限制性原则，以平衡对外开放和国家安全的双重目标，为全球数据治理提供了审慎包容、鼓励合作的中国方案。不过，数据自由流动与数据安全流动的冲突并不会自然消解，其有赖于不同数据跨境类型下的原则权衡。

https://mp.weixin.qq.com/s/T_sBH6U9fGG9zwPbc-mCow

4. 数据安全范式革新及其立法展开

数字经济时代数据大规模的流动、聚合和分析带来了新的风险与挑战，信息安全和网络安全范式已经不足以应对，维护数据安全亟需范式革新。应该建立以数据风险管控为中心的数据安全范式：除了包括传统数据自身安全的保密性、完整性、可用性，还要确保数据利用安全的可控性和正当性。

对于数据安全立法而言，要从国家安全高度进行数据安全法制体系化设计，以风险管控为中心构建数据安全保护制度体系，以重要数据安全为核心管控国家数据安全风险。特别是在制度建构上，应该以重要数据为抓手构建国家数据安全管理制度，包括明确重要数据的识别认定制度、规定重要数据处理者的安全保护义务、将重要数据安全审查纳入网络安全审查以及建立重要数据出境管制制度。

https://mp.weixin.qq.com/s/zQ2hj0c6_wWqaNRuE7cr5A

5. 2020-2021 年度数字经济形势分析

2020 年，疫情凸显数字经济发展韧性的同时，也显现了不少发展过程中存在的问题与挑战。“数据孤岛”制约数据要素价值开发利用，数字鸿沟由“接入鸿沟”向“能力鸿沟”演变，数字经济国际规则对企业海外权益保障有效性不足，数字经济测度体系的“宽”“窄”口径均亟待完善。展望“十四五”，数字经济将保持快速、持续、健康发展，成为未来经济发展“主形态”，我国作为全球数字经济第二大国，有望实现增速领跑。分领域看，算力基础设施对经济社会发展的支撑作用不断扩大，数据交易在“区块链+隐私计算”等新技术推动下将会实现破局，政府、企业、个人的数字理解、使用和技能水平都将极大提升。

https://mp.weixin.qq.com/s/L43TWvvY9AxhT0dalXYRLg

6. 安全基线建设指南

安全基线=安全能力+安全能力上配置的安全策略。在建立事件响应机制之前，必须存在基础的能力。这些基础能力用于保障数字资产/业务的**可用性、保密性、完整性**。安全基线是为业务系统生成的。**安全基线应该根据企业战略、业务属性生成，每个企业、每种不同类型的资产的基线都不一样**。安全基线应该由业务团队和安全团队共同参与，并且其中有大量的内容和工作是依靠人力施行的，包括：**资产清点、评估业务内部和外部的风险、确定业务影响的范围、人员职责和意识的培训**等。但同时也是有很多可以通过信息化手段进行管理的内容，包括：**资产清点、分类、识别并记录资产漏洞、建立访问控制策略、数据保护策略、建立完整性检查机制**等。更为重要的是安全基线不仅是给人看，它也是“威胁分析”和“事件响应”过程中的重要输入。所以需要建设一套安全基线配置系统对资产的基线进行可视化的管理。

https://mp.weixin.qq.com/s?__biz=MzI4NDY2MDMwMw==&mid=2247495169&idx=1&sn=50e49914cb0cad3123167c02aa972afd

7. 同态加密：密码学的下一个黄金时代

现代加密方式已经嵌入无数的数字系统和组件，成为保护数据安全性和隐私相关的必要工具。但是密码学现在最大的限制，在于需要处理和分析敏感数据的时候必须进行解密。然而，包括医疗、法律、制造商、金融和在线选举等在内，有大量的领域需要对数据进行分析处理；如果能不使用加密密钥就直接对数据进行分析，就能达成目标的同时，还能确保数据的隐私性。

这就产生了同态加密的概念。同态加密使用基于格加密的算法来隐藏输入值、中值、输出值，甚至函数本身可以让任何没有密钥的人进行计算。换而言之，**同态加密可以直接使用于加密数据**。尽管说全同态加密（FHE）才诞生了十年多，伴随强大算力的计算机和更好的算法，使得全同态加密得以落地。

https://mp.weixin.qq.com/s/mzOGR5kX7y8DLAk38p9KGg