全球数据安全观察

总第 121 期 2023 年第 2 期

(2023.01.09-2023.01.15)

大数据协同安全技术国家工程研究中心

NERCBDS
大数据协同安全技术
国家工程研究中心

目录

政策形势

1、工业和信息化部等十六部门发布《关于促进数据安全产业发展的指导意见》

1 月 13 日，工业和信息化部等十六部门发布《关于促进数据安全产业发展的指导意见》，明确了数据安全产业发展的指导思想和基本原则，提出了至 2025 年、2035 年分别需要实现的发展目标，并基于此确定了七大重点任务：**提升产业创新能力、壮大数据安全服务、推进标准体系建设、推广技术产品应用、构建繁荣产业生态、强化人才供给保障、 深化国际交流合作**。

https://www.miit.gov.cn/jgsj/waj/wjfb/art/2023/art_e92c30f708884a3db7a77e135682ea8b.html

2、中国银保监会发布《银行保险监管统计管理办法》

2022 年 12 月 25 日，中国银保监会发布《银行保险监管统计管理办法》，包括总则、监管统计管理机构、监管统计调查管理、银行保险机构监管统计管理、监管统计监督管理和附则等六章，就**明确归口管理要求、明确数据质量责任、明确数据质量责任、对接数据治理要求、重视数据价值实现**等内容作出规范。

http://www.cbirc.gov.cn/cn/view/pages/govermentDetail.html?docId=1089714&itemId=861&generaltype=1

3、上海市经济信息化委、市互联网信息办公室印发《上海市公共数据开放实施细则》

2022 年 12 月 31 日，《上海市公共数据开放实施细则》印发，从总体原则、数据开放、数据获取、信息系统与开放平台、数据利用等方面明确了公共数据开放的实施要求，以促进公共数据更深层次、更高水平开放。

http://sheitc.sh.gov.cn/sjxwxgwj/20230110/cc487968a94849618ee9374618e53673.html

4、《临港新片区国际数据产业专项规划（2023-2025 年）》印发

1 月 5 日，中国（上海）自由贸易试验区临港新片区管理委员会印发《临港新片区国际数据产业专项规划（2023-2025 年）》，结合临港新片区数字经济发展定位、产业布局、城市空间布局，提出了**构筑数据要素支撑底座、打造数据产业承载区、构建繁荣有序市场生态、推进跨境数据流动服务、提升数据赋能产业价值**五大主要任务。

https://www.lingang.gov.cn/html/website/lg/index/government/fi

le/16114261247111045l4.html

5、北京市通管局：通报 29 款存在隐私合规和网络数据安全问题的 APP

1 月 11 日，北京市通信管理局对存在侵害用户权益和安全隐患等问题的 29 款 App 作出通报，其中 21 款 App 存在未经用户同意收集使用个人信息、违规向他人提供个人信息、未对敏感用户数据进行加密、强制用户使用定向推送以及未明示收集使用个人信息的目的、方式和范围等不同类型问题而被通报整改；8 款 App 则涉及账号注销难、未经用户同意收集使用个人信息等问题，因问题整改不到位被下架处置。

https://bjca.miit.gov.cn/zwgk/tzgg/art/2023/art_b8c68f14f8cf48b5b1491dd0513e2030.html

6、广州数据交易所行业数据指数公开发布

1 月 13 日，全国首个数据交易领域的行业数据指数发布平台上线，涵盖 10 个行业 80 余项行业数据指数集中发布。该平台将为各行业提供权威数据指数发布渠道，并以行业数据指数为牵引，引导各方力量共同构建数据交易新格局，带动整个行业数据交易生态的创新发展。

http://zfsg.gd.gov.cn/xxfb/ywsd/content/post_4081458.html

技术、产品与市场

1、IDC 发布数字政府数据安全领导者实践报告

IDC 观察到，数字政府数据安全建设中，引入了很多新技术、新模式、新体系。例如，利用云化、服务化实现安全大规模建设的集约共享，利用工具及人工智能技术进行数据梳理及分类分级，利用大数据、机器学习和 UEBA（用户和实体行为分析技术）技术对流转中的数据交互进行审计和稽核，从组织、制度、流程、技术几个维度进行数据安全体系建设，通过建设数据安全常态化运营体系提升组织整体的安全能力等。

IDC 认为，数字政府在进行数据安全建设时，需要从以下几点考量:

（1）建立针对数据安全的组织制度。数据安全建设不能局限于网络安全的视角，建立数据安全组织和管理制度，对日常的数据安全管理工作进行相关约束，从网络安全合规演进到数据安全合规。

（2）进行数据治理，有效梳理数据资产和进行分类分级。通过网络扫描和数据库的遍历查询，自动梳理数据资产清单，基于机器学习实现字段与分类分级标准的映射，实现智能数据分类分级。

（3）云化、服务化实现安全大规模建设的集约共享。通过采用高集约化的云融合密码服务模式， 提供了满足云时代分层解耦的安全服务能力。通过云化集中管控海量设备和资源，策略更新自动下发，实现安全的统一防护，安全数据的可视化，为大规模部署提供了可能。

（4）利用大数据和人工智能技术实现数据流转中的泄漏分析和溯源。通过用户和资产画像，对数据共享开放过程中的数据交互行为进行审计和稽核，实时感知数据异常和潜在风险，结合数据流转实时地图，进行数据泄露的溯源。

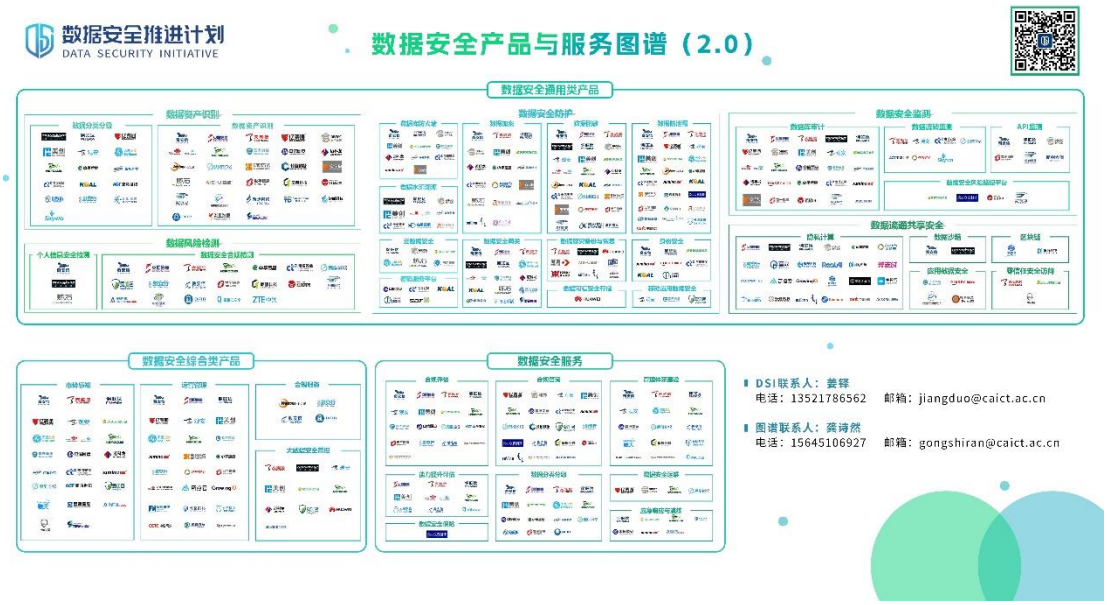
（5）汇聚各类数据，建设数据安全运营体系。对各层面环节的数据安全统一策略防护和管控，建设一体化运营平台，实现业务敏感数据的规范化、标准化和常态化管理，推动数据安全管控目标的落地。

https://www.secrss.com/articles/50866

2、《数据安全产品与服务图谱（2.0）》正式发布

为深化调研我国数据安全产品与服务市场现状，《数据安全产品与服务图谱 2.0》（以下简称“图谱 2.0”）在原图谱框架的基础上实现了更具体系化、层次化的升级迭代，旨在进一步打通供需双方对当前主流数据安全产品与服务的认知，洞察数据安全市场的发展趋势。

经过三个月的征集统计，图谱 2.0 合计收录 116 家企业的 488 款数据安全产品及服务信息，将数据安全产品与服务分为数据安全通用类产品、数据安全综合类产品、数据安全服务三大类别。其中，数据安全通用类产品覆盖了数据资产识别、数据风险检测、数据安全防护、数据安全监测、数据共享流通安全五大领域，数据安全综合类产品聚焦态势感知、运营运维、合规服务、大数据安全管控等方向，提供常态化、一体化的数据安全能力，数据安全服务则关注数据安全合规、数据安全能力提升等内容。



https://mp.weixin.qq.com/s/31yKcBVbkkBGClrEOj3Ksg

3、《2022 年数据安全行业调研报告》正式发布

《2022 年数据安全行业调研报告》是数据安全推进计划

通过问卷的方式分别对数据安全需求侧与供应侧的数据安全发展现状进行调研，并形成的报告，旨在梳理数据安全行业建设现状，形成数据安全行业整体视图。

根据本次调研结果，参与调研的需求侧企业均不同程度的开展了数据安全工作并制定了数据安全工作规划，供应侧厂商也认为数据安全市场前景非常广阔，并积极布局数据安全产品及服务。

综合来看，我国数据安全已迈入飞速发展的关键时期，需求侧数据安全投入占比持续走高，需求量上升，在给供应侧带来发展机遇的同时，也对数据安全服务质量与产品技术能力提出了更高的要求。

https://mp.weixin.qq.com/s/SGSKOqFAa8SdfbO3HGqCzA

4、中国信通院发布《数据要素流通视角下数据安全保障研究报告（2022 年）》

报告围绕数据要素流通视角下流通数据、流通活动、流通设施的安全需求，分析健全我国数据安全保障体系的推进思路，并从分类分级、流通环境、安全技术、协同共治等方面提出措施建议，为完善我国数据要素流通视角下数据安全保障提供有益参考与借鉴。

报告核心观点如下：（1）数据安全内涵不断延展；（2）流通数据形态逐步拓展，数据分类分级难度加大；（3）数据流通路径复杂主体多元，增加“后链路风险”；（4）数据流通设施开放互动增强，安全保障压力倍增；（5）国内外积极探索平衡数据流通利用与安全保护；（6）面向数据流通全链条各主体，分步有序地构建数据安全保障体系。

https://mp.weixin.qq.com/s/3i4zGGYtbr9g2QeHpBxIOA

5、隐私计算入选 2023 年十大科技趋势预测

近日，百度研究院发布“2023 年十大科技趋势预测”，隐私计算被列为十大科技趋势之一。分析认为，深度学习平台加大模型，构筑了坚实的产业智能化基座，会进一步加速产业智能化升级。数实融合，为技术底座的夯实提供了强大动力和广阔市场空间。隐私计算，成为支撑数据安全治理和

数据要素市场化发展的重要基石。数据安全治理和数据要素市场化的重要性和紧迫性日渐上升，隐私计算技术进入快速发展阶段，金融、通信、医疗、互联网等领域有越来越多的机构开始自建隐私计算平台，应用场景不断拓展和深化，推进各家隐私计算平台的互联互通逐渐成为行业新趋势。在此背景下，横纵交织的可信数据流通网络初步呈现。可以预见，借助不断发展壮大的数据流通网络，未来几年隐私计算技术的应用场景将会不断推陈出新，隐私计算平台也会在多个行业成为支撑数据安全治理和数据要素市场化发展的重要基石，有助于塑造兼顾价值创造和安全可信的数据产业。

https://mp.weixin.qq.com/s/ZD6yNwU1G0KqIEJVcpruxw

业界观点

1、何强：构建中国式现代化的数据治理体系，离不开完善的国家数据治理框架

1 月 6 日，第七届新金融论坛在北京举行。国家统计局统计科学研究所党委委员、首席统计师何强出席论坛并发表演讲。

何强指出，需要建立一个国家数据治理政策框架，充分利用数据的力量，来建设更有效运行的数字政府，实现更大的公共利益，做出更具引领性的创新。为此，需要从**明晰国家高层政策意图、夯实数据基础架构和标准、明晰国家高层政策意图**以及**深入推进数据整合、共享和可获取性**四个方面进行着手，对此他做出了详细的阐述。

何强总结，构建中国式现代化的数据治理体系，离不开完善的国家数据治理框架。完善的国家数据治理框架，应当明晰国家高层政策意图，夯实数据基础架构和标准，有效实施数据托管和管理，以及深入推进数据整合、共享和可获取性。在国家数据生态系统迅速扩张的过程中，包括金融机构、统计机构、互联网监管机构等在内的很多数据利益攸关方的职能和功用，将会被重新界定，进而加速推进国家治理的数字化、数据化和数智化。

http://www.echinagov.com/viewpoint/334688.htm

2、汪玉凯：数据治理是智慧城市治理现代化的关键

党的二十大报告提出，要“加强城市基础设施建设，打造宜居、韧性、智慧城市”。中央党校（国家行政学院）教授、国家信息化专家咨询委员会委员汪玉凯认为这对智慧城市建设提出了新的要求。

他指出，当前智慧城市治理现代化建设呈现出以下方向：一是城市治理现代化必须坚持“三化方向”，即科学化、精细化、智能化；二是城市治理现代化的价值主要包括三方面：人本性、公共性、协同性。

汪玉凯提出智慧城市建设发展要有问题导向、问题意识，他明确了数据治理能力在城市现代化过程中的意义，并认为当前，智慧城市建设中公共数据治理方面存在以下三个问题：一是在实现从三难、三通到三跨的目标时，数据治理成为瓶颈；二是我国公共数据治理主要存在“三低”现象，即整合度比较低、共享度低、开放度低；三是公共数据的治理难点不是技术问题，而是权力问题，存在部门利益壁垒。

对此，汪玉凯认为可从以下四个方面考虑提升我国公共数据的治理能力有何路径：

一是加强智慧城市建设中公共数据基础设施的统筹，防

止重复建设，特别要注重改变观念，提高数据治理能力。

二是通过改革加大公共数据改革的力度，提高公共数据资源的共享度。

三是要制定严格的制度，保障公共数据资源的开放。

四是在实践中探索将部分公共数据资源通过市场交易的方式开放，实现双赢。

http://www.echinagov.com/viewpoint/334686.htm

3、林琳：数据交易如何更规范高效

2021 年以来，国家相关政策、法律法规等密集出台，各地积极探索，截至 2022 年 8 月，已有 40 多家数据交易场所成立。数据交易场所建设如火如荼，为解决交易过程中的效率、合规、安全、信任等问题提供了重要平台，但也面临数据产权不清、新技术支撑不充分、出现同质化竞争苗头等情况，对此还需各个击破。

确权是基础。从实践来看，公共数据和个人数据的权属问题相对清晰，企业数据方面则较为复杂。当前，一些数据交易场所已逐步形成数据登记等确权模式，迈开了破解“确权难”的第一步。从长远来看，根据数据来源和数据生成特征，国家层面的公共数据、企业数据、个人数据分类分级确权授权制度亟待建立，通过分别界定数据生产、流通、使用过程

中各参与方享有的合法权利，为激活数据要素价值创造和价值实现提供基础性制度保障。

技术是支撑。数据需要流通才会产生价值，但由于数据具有可复制性等特点，在交易中容易发生所有权交接不清楚、隐私泄露等问题，反而阻碍了流通。破解两难，技术支撑必不可少。在清洗加工等环节，针对交易数据尤其是高敏感度和高价值数据，可通过隐私计算来进行分析、建模。在数据调用等环节，区块链技术有利于实现全链条监管，上海数据交易所已经采用联盟链将与交易有关的信息存储在区块链节点中，提高了交易的安全可信度。在对数据泄露的溯源和追责方面，数据水印技术可将标识信息隐藏在结构化数据中，对溯源取证提供了有力支持。下一步，还需加大这些技术的研发创新、标准完善和应用推广，为数据流通插上安全的翅膀。

布局需优化。目前，华东、华南、华中地区的数据交易场所占比达 70%，有的单一省份已设立了 5 家。为了避免区域分割和同质化竞争，主管部门需加强数据交易场所体系设计，统筹优化规划布局，引导多种类型的数据交易场所共同发展，构建多层次市场交易体系，推动区域性、行业性数据流通使用。数据交易场所自身也有必要找准优势，错位发展，提高数据要素供给数量和质量，延展出市场所需的数据产品

和服务。

http://cbdio.com/BigData/2023-01/09/content_6171574.htm

4、江小涓、白京羽：构建数据基础制度体系的有力举措

与传统生产要素相比，数据要素具有产权复杂性、交易多元化、技术依赖性强等特征。《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”）既把握数据同其他生产要素的共性，又把握数据要素的特性，提出了有针对性的措施。

处理好数据产权和使用权的关系。“数据二十条”并不回避数据要素的复杂产权问题，同时更强调使用权，提出“探索数据产权结构性分置制度”，要求“根据数据来源和数据生成特征，分别界定数据生产、流通、使用过程中各参与方享有的合法权利”，从而在总体框架上采用结构性分置，具体操作上采用分类分级确权授权使用，创造性提出建立数据资源持有权、数据加工使用权和数据产品经营权“三权分置”的数据产权制度框架，构建中国特色数据产权制度体系。这既符合社会认知基础、数据要素特点、事物发展规律，也为今后继续探索留下足够空间。

处理好场内交易和场外交易的关系。“数据二十条”提出“完善和规范数据流通规则，构建促进使用和流通、场内场外

相结合的交易制度体系，规范引导场外交易，培育壮大场内交易”，并在完善数据全流程合规与监管规则体系、统筹构建规范高效的数据交易场所、培育数据要素流通和交易服务生态等方面提出指导意见，为探索建立合规高效、场内场外结合的数据要素流通和交易制度指明了前进方向，也有利于探索更优的数据交易方式。

处理好数据共享和数据安全的关系。“数据二十条”对公共数据的开发利用作出规定，主基调是坚持开放共享，强调“推进实施公共数据确权授权机制”，鼓励公共数据在保护个人隐私和确保公共安全的前提下，按照“原始数据不出域、数据可用不可见”的要求，以模型、核验等产品和服务等形式向社会提供，对不承载个人信息和不影响公共安全的公共数据，推动按用途加大供给使用范围。也要看到，可以无条件开放的公共数据是有限的，大部分公共数据具有一定敏感性。在这方面，“数据二十条”要求“依法依规予以保密的公共数据不予开放，严格管控未依法依规公开的原始公共数据直接进入市场，保障公共数据供给使用的公共利益”。这些规定为在确保数据安全的前提下，最大限度促进公共数据的高效利用和要素价值释放提供了有力制度保障。

数据的大规模流通应用对数据安全相关技术创新发展提出了更高要求。“数据二十条”高度重视数据安全相关技术

创新发展，鼓励探索数据流通安全保障技术、标准、方案；支持开展数据流通相关安全技术研发和服务，促进不同场景下数据要素安全可信流通；提出以“揭榜挂帅”方式支持有条件的部门、行业加快突破数据可信流通、安全治理等关键技术。这对于实现以数据安全技术保障数据合理使用、以数据使用促进数据安全技术持续发展具有重要推动作用。

https://digital.gmw.cn/2023-01/10/content_36291273.htm

5、周民：完善数据要素治理制度，保障数据流通交易安全

《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称《数据二十条》）明确了把握数据要素治理的三个“着眼点”：（一）“保安全”：数据安全是数据要素流通交易的底线；（二）“重发展”：发挥政府有序引导和规范发展的作用；（三）“促创新”：对于探索性创新的领域建立容错机制。

《数据二十条》从构建新发展格局、推动高质量发展的战略高度，统筹考虑政府、企业和社会三方职责，重点下好数据流通交易三步“先手棋”：（一）建立监管机制，创新政府数据治理思路；（二）压实企业责任，推动企业积极参与治理；（三）强化多元协同，发挥社会力量协同治理。

数据要素基础制度立足我国数字经济发展现状，针对数据流通交易中的确权难、监管难等问题，构筑起防范数据流

通交易风险的三道“安全线”:

（一）完善制度设计

解决数据要素安全治理问题，要从完善制度规则等方面入手，重点做好三方面工作。一是推动完善适用于不同主体多元共治的治理体系，明确不同类型数据的权责主体，完善数据不同场景的使用规则和法律法规，对于不适于流通交易的数据，制定完善的开放和保密准则。二是建立健全数据交易安全标准规范和安全制度体系，制定数据隐私保护和安全审查制度，加强对政务数据、企业商业秘密和个人数据的隐私与安全保护。三是完善平台类企业数据管理制度，制定平台企业在数据迁移、交易和处置等方面的制度规则，营造规范有序、包容审慎的数据要素生态体系。

（二）鼓励多方协同

坚持以人民为中心的发展思想，充分发挥、企业、社会组织各参与主体的积极性、主动性。政府应从完善法律法规、优化制度设计入手，通过媒体和社会组织对特定行业、产品和服务的数据安全治理状况实施社会监督，督促企业在开发数据产品和服务时提升数据安全意识，依据法律法规和行业数据标准及时提升数据安全防护能力。企业应积极承担社会责任，在数据安全基础设施建设、日常管理、技术研发等方面积极发挥作用，走好数据安全治理的“最后一公里”。社会

组织作为生态体系中的重要一环，应在合规公证、安全审计、算法审查、监测预警、风险评估和人才培养等方面发挥作用。

（三）强化技术创新

破解数据流通交易的中数据安全问题，要充分应用区块链、隐私计算等技术，从隐私保护技术、安防监管方面进行化解。一是利用区块链、隐私计算等新型技术实现数据“可用不可见”，有效管控数据计算价值使用的目的和方式，实现数据使用的事前评估和持续监督相结合、风险自评估与安全监督相结合，保障数据使用的安全与合法，破解数据滥用、隐私泄露、用户歧视等问题。二是改进提高监管技术和手段，依托大数据技术建立健全违法线索线上发现、流转、调查处理等机制，提升分析预警、线上执法、信息公示等监管能力。同时，鼓励条件成熟的地区开展试点创新，以点带面提高数据交易流通安全保障能力。

https://www.ndrc.gov.cn/xxgk/jd/jd/202212/t20221219_1343659.html

数据安全事件

1、旧金山湾区地铁遭勒索攻击，轨交业已成黑客攻击重灾区

1 月 10 日消息，在被勒索软件团伙公开列入“已勒索”名单后，旧金山湾区城轨交通系统（BART）开始对这起疑似勒索事件开展调查。

作为美国第五繁忙的重轨快速交通系统，BART 在 1 月 6 日被列入 Vice Society 勒索软件团伙的泄密网站上。BART 首席通讯官 Alicia Trost 表示，他们正在调查该团伙窃取和发布的数据。

她称，“需要明确的是，BART 的服务或内部业务系统并未受到影响。与其他政府机构一样，我们正采取一切必要的防范措施加以应对。”

https://www.secrss.com/articles/50929

2、推特否认黑客指控，保证泄露的用户数据不是来自其系统

1 月 12 日，据外媒报道，推特在一份声明中表示：“根据调查的信息和情报分析，没有证据表明泄露的数据是通过利用 Twitter 系统的漏洞获得的。”“这些数据很可能是已经通过不同来源在线公开的数据集合。”

此前有多份报告称，属于数百万用户的 Twitter 数据

（2022 年 11 月为 540 万，2022 年 12 月为 4 亿，上周为 2 亿）已在在线犯罪论坛上出售。

这家社交媒体巨头进一步表示，该漏洞“与之前报道的事件无关，也与任何新事件无关”，并补充说没有密码被泄露。据说 12 月和 1 月发布的两个数据集是相同的，后者删除了重复的条目。

https://thehackernews.com/2023/01/twitter-denies-hacking-claims-assures.html

3、《卫报》称黑客访问了英国员工数据

1 月 11 日报道，《卫报》称，2022 年 12 月下旬导致英国报纸关闭其办公室数周的网络事件是由勒索软件引起的，并于周三通知员工黑客已经访问了他们的数据。

据称，此次攻击很可能是由一封网络钓鱼电子邮件引发的，该报没有提供暴露数据的详细信息，但它澄清说，其美国或澳大利亚办事处的读者或员工的个人数据没有受到影响。

https://www.inforisktoday.com/guardian-says-hackers-accessed-uk-employee-data-a-20911

4、法航和荷航部分客户个人信息被盗

1 月 9 日报道，据 Bleeping Computer 网站披露，法航和荷航已经通知“蓝天飞行”的旅客，他们的一些个人信息可能被网络犯罪分子盗取了。

在发给旅客的通知中，法航和荷航表示内部安全运营团队检测到一个未经授权的攻击活动，可能造成用户信息泄露，目前已经采取了防御措施，以防止用户数据进一步暴露。

据悉，泄露的用户数据信息主要包括旅客的姓名、电子邮件地址、电话号码、最新交易和蓝天飞行的信息（例如旅客所赚取的里程余额）。值得一提的是，航空公司表示此次攻击事件没有暴露客户的信用卡或支付信息，但受影响的客户账户因网络攻击事件被锁定了，必须到荷航和法航的网站上更改密码。

https://www.freebuf.com/news/354694.html

5、社交市场 Trustanduse 暴露了近 50 万用户的数据

1 月 12 日，Cybernews 研究团队发现了一个可公开访问的数据库，其中存储了多达 855GB 的敏感用户和业务数据，这些数据属于社交市场 trustanduse.com。

被发现的数据库包括敏感数据，例如用户名、个人全名、Facebook ID、电话号码和使用 BCrypt 算法散列的密码等。

研究人员表示，当犯罪者使用窃取的帐户凭据未经授权访问其他系统上的用户帐户时，撞库攻击不太可能发生。然而，威胁行为者可以将这些数据用于垃圾邮件和鱼叉式网络钓鱼活动，最常见的形式是试图欺骗受害者，让他们支付金钱或获取更多有价值的信息。

https://securityaffairs.com/140678/data-breach/trustanduse-data-leak.html?web_view=true

6、数据泄露暴露了 10,000 名法国社会保障受益人的信息

1 月 10 日，据外媒报道，在将包含个人信息的文件发送给服务提供商后，法国社会保障机构 CAF 的 10,000 多名受益人发现他们的数据暴露了大约 8 个月之久。

调查发现，位于吉伦特省的 CAF 向负责培训该组织统计人员的服务提供商发送了一份包含 10,204 名受益人的敏感和个人信息的文件。

供应商否认曾要求使用真实信息，而吉伦特 CAF 显然未能具体说明发送的数据包括当前受益人的信息。泄露的个人信息包括地址（号码和街道名称）、出生日期、家庭构成、收入金额和领取福利的类型等。

CAF 忽略了个人数据匿名化的基本原则，这种数据传输揭示了 CAF 对个人数据的漠视。法国数据保护机构 CNIL

很可能会发起详细调查，CAF 最终可能会因违反 GDPR 而导致制裁。

https://www.csoonline.com/article/3685233/data-leak-exposes-information-of-10-000-french-social-security-beneficiaries.html?&web_view=true

7、健康保险公司 Aflac 指责美国合作伙伴泄露日本客户保单信息

1 月 11 日，据外媒报道，全球保险公司 Aflac 的日本分公司透露，其癌症保险产品超过 300 万客户的个人数据已在网上泄露。

该公司已向客户道歉，并承认他们的姓氏、年龄、性别和保险范围都被泄露了。但保险公司声称泄露的数据没有足够的信息来识别个人客户，并将滥用的可能性评为“极低”。

尽管如此，这一违规行为还是值得注意的，因为 Aflac 将此事件归咎于一家美国承包商，该承包商的服务器从 1 月 7 日开始受到未经授权的访问。

https://www.theregister.com/2023/01/11/japan_aflac_zurich_data_breaches/?&web_view=true

8、Vice Society 勒索软件声称对澳大利亚消防服务进行了攻击，造成数据泄露

1 月 12 日，据外媒报道，澳大利亚维多利亚消防救援队(FRVP)披露了 12 月网络攻击造成的数据泄露事件，现在 Vice Society 勒索软件团伙已承认该数据泄露事件。

“该事件影响了我们的许多内部服务器，包括我们的电子邮件系统，”FRV 在其网站上的公告中说明。除了破坏该机构的 IT 系统外，黑客还窃取了 FRV 计算机的数据，包括有关现任和前任雇员、承包商、借调人员和求职者的信息。根据已公开的部分通知，黑客窃取了以下信息：全名、地址、电子邮件地址、电话号码、出生日期、银行账户详细信息、护照资料、税号等等。除了上述之外，由于黑客访问了该机构的电子邮件系统，他们还可能访问或窃取了敏感的电子邮件通信。

https://www.bleepingcomputer.com/news/security/vice-society-ransomware-claims-attack-on-australian-firefighting-service/

9、英国邮政公司 Royal Mail 透露其遭到 LockBit 勒索攻击

1 月 12 日，据报道，英国最大的邮政服务 Royal Mail 遭到与 LockBit 勒索软件有关的攻击。1 月 11 日，Royal Mail 透露称其遭到了网络攻击，国际航运服务受到了影响。虽然

该公司并未透露关于攻击的任何细节，但《每日电讯报》在1月12日报道称，目前已确认攻击来自 LockBit，或者有攻击者使用了他们的加密程序。攻击活动加密了国际运输的设备，并在用于海关备案的打印机上打印赎金记录。

https://www.bleepingcomputer.com/news/security/royal-mail-cyberattack-linked-to-lockbit-ransomware-operation/

10、法国 CNIL 因违反 cookie 法对 Tiktok 罚款 540 万美元

1月14日报道，国家信息和自由委员会 (CNIL) 因违反 cookie 同意规则而对短视频托管服务 TikTok 处以 500 万欧元（约合 540 万美元）的罚款。法国数据保护监管机构声称，用户无法拒绝 cookie，就像他们接受 cookie 一样容易，字节跳动旗下的公司也未能充分告知不同 cookie 的目的。CNIL 认为，让拒绝机制更复杂实际上相当于阻止用户拒绝 cookie，并鼓励他们更喜欢“全部接受”按钮的便利性。这一过程侵犯了互联网用户的同意自由，构成了违反《数据保护法》第 82 条的行为。

https://securityaffairs.com/140786/digital-id/cnil-fined-tiktok.html?_ga=2.107486341.68580306.1673779871-

556034239.1631001578&_gl=1*18ez4no*_ga*NTU2MDM0MjM5LjE2MzEwMDE1Nzg.*_ga_P62M3QN974*MTY3Mzc3OTg3MS43Ni4wLjE2NzM3Nzk4NzEuMC4wLjA.*_ga_8ZWTX5HC4Z*MTY3Mzc