全球数据安全观察

总第 127 期 2023 年第 8 期

(2023.02.27-2023.03.05)

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、中共中央 国务院印发《数字中国建设整体布局规划》

2 月 27 日，中共中央、国务院印发《数字中国建设整体布局规划》，明确，数字中国建设按照“2522”的整体框架进行布局，即夯实数字基础设施和数据资源体系“两大基础”，推进数字技术与经济、政治、文化、社会、生态文明建设“五位一体”深度融合，强化数字技术创新体系和数字安全屏障“两大能力”，优化数字化发展国内国际“两个环境”。

http://www.gov.cn/xinwen/2023-02/27/content_5743484.htm

2、工业和信息化部发布进一步提升移动互联网应用服务能力的通知

近日，工业和信息化部印发通知以进一步提升移动互联网应用服务能力，共提出 26 条措施：围绕“**提升全流程服务感知，保护用户合法权益**”方面，聚焦规范 APP 安装卸载、服务体验优化、个人信息保护强化、诉求响应等提出 12 条措施；围绕“**提升全流程服务感知，保护用户合法权益**”方面，聚焦 APP 开发运营者责任落实、平台分发管理强化、SDK 规范、终端安全防线筑牢和接入企业责任夯实提出 14 条措施。

http://www.gov.cn/zhengce/zhengceku/2023-

03/02/content_5744106.htm

3、上海市通信管理局发布开展“浦江护航”2023 年电信和互联网行业数据安全专项行动的通知

2 月 28 日，上海市通信管理局发布开展“浦江护航”——2023 年电信和互联网行业数据安全专项行动的通知，提出试点实施电信和互联网行业首席数据官制度、开展重要数据和核心数据识别认定及目录管理、开展电信和互联网行业数据安全风险评估管理、开展常态化数据安全监测预警与通报处置、加强企业数据全生命周期安全管理、加强数据安全能力建设和人才培养六项重点任务。

https://mp.weixin.qq.com/s/kn8mdCJLsV8CidPttmCWDA

4、《深圳市数据交易管理暂行办法》《深圳市数据商和数据流通交易第三方服务机构管理暂行办法》印发

3 月 2 日，深圳市发展和改革委员会发布《深圳市数据交易管理暂行办法》、《深圳市数据商和数据流通交易第三方服务机构管理暂行办法》。前者明确了对数据交易主体、数据交易场所运营机构、数据交易标的、数据交易行为、数据交易安全等方面的要求，后者围绕数据商和数据流通交易第三方服务机构的业务运行、安全管理、监督管理等方面作出要

求。

http://www.sz.gov.cn/cn/xxgk/zfxxgj/zcfg/content/post_10454883.html

http://www.sz.gov.cn/cn/xxgk/zfxxgj/zcfg/content/post_10454838.html

5、《新疆维吾尔自治区公共数据管理办法（试行）》发布

2 月 22 日，新疆维吾尔自治区人民政府办公厅发布《新疆维吾尔自治区公共数据管理办法（试行）》，明确了公共数据管理的总体原则、公共数据目录、公共数据采集与归集、公共数据共享、公共数据开放、公共数据安全等方面的要求。

http://www.xinjiang.gov.cn/xinjiang/c112545/202302/95dd5c4e77a5457ba54907787b26dbf7.shtml

6、美国发布 2023 年版《国家网络安全战略》

3 月 2 日，美国正式发布发新版《国家网络安全战略》，详细阐述了拜登政府网络安全政策将采取的全方位措施。其中，围绕建立“可防御、有韧性的数字生态系统”的内容，具体涉及保护关键基础设施、破坏和摧毁威胁行为者、塑造市场力量以推动安全和韧性、投资于韧性未来、建立国际伙伴关系以追求共同目标 5 大支柱的 27 项举措。

https://www.secrss.com/articles/52462

技术、产品与市场

1、2022 年度数据安全行业十大观察

为更好地观察数据安全需求侧数据安全建设现状与面临的挑战，了解供应侧数据安全业务布局与产品服务技术形态，数据安全推进计划（DSI）联合中国通信标准化协会大数据技术标准推进委员会（CCSA TC601）联合发布了《2022 年数据安全行业调研报告》。基于调研报告，本文梳理了 2022 年数据安全行业十大观察，具体如下：

(1) 数据安全意识及能力逐步提高；

(2) 以数据为中心建设数据安全防护能力；

(3) 企业亟待建设“多方联合”的数据安全组织架构；

(4) 数据分类分级在数据安全治理中率先落地；

(5) 人才培养是未来一年应用方企业的重点工作内容；

(6) 数据安全供应侧企业呈现三种形态；

(7) 安全合规、数据安全体系建设成为数据安全服务布局热点；

(8) 数据分类分级产品技术及配套服务蓬勃发展；

(9) 数据安全培训服务具备市场拓展空间；

(10) 第三方评测助力厂商创造新优势。

https://mp.weixin.qq.com/s/iSlJwJfRtZcfU0SqJtfzfA

2、《2022 年数据资产泄露分析报告》：超 3200 起，涉及金融物流电商等行业

大数据、互联网为企业带来无限发展生机的同时，也暗藏了巨大的数据安全隐患。伴随数字化转型深入发展，数据泄露事件的频率、规模和成本也较往年有所上升，对企业造成了持续、难以消弭的影响。

威胁猎人《2022 年数据资产泄露分析报告》基于过去 1 年捕获到的数据泄露事件，结合数据安全现状，多维度呈现 2022 年国内数据泄露的态势全景。报告有如下发现:

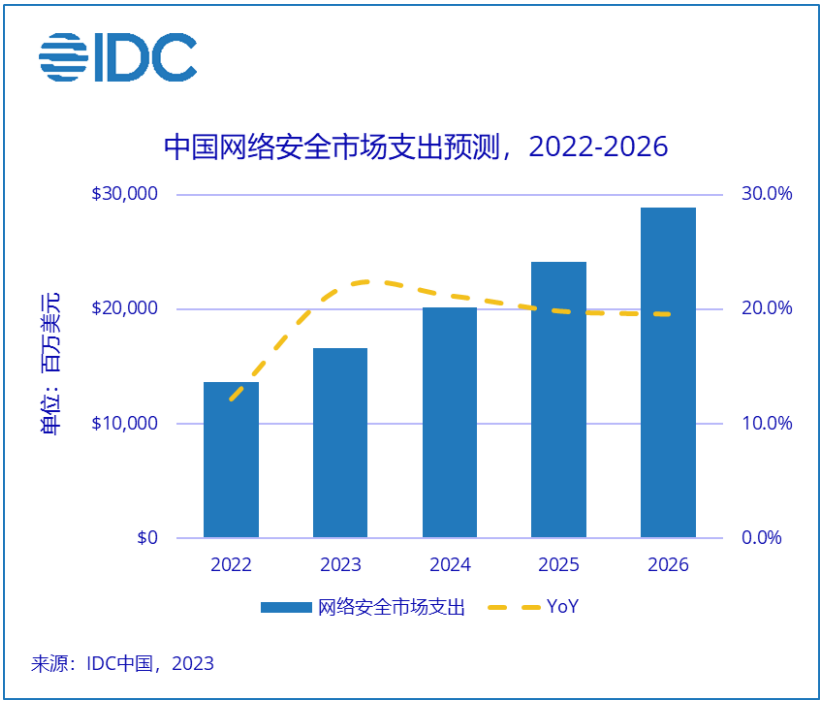
- 2022 年累计捕获数据泄露事件超 3200 起，较 2021 年上升近一倍。
- 数据泄露渠道来源广泛，匿名社交软件占比超 75%。
- 2022 年数据泄露行业分布中，金融、物流、电商行业占据前三。
- 2022 年数据泄露主要原因中，运营商通道泄露占比第一。

https://www.sohu.com/a/648860293_100109628

3、中国网络安全相关支出将以 18.8%的年复合增长率增长，增速位列全球第一

IDC 数据显示，2022 年全球网络安全总投资规模为 1,955.1 亿美元，并有望在 2026 年增至 2,979.1 亿美元，五年复合增长率（CAGR）约为 11.9%。

聚焦中国市场，部分终端用户受疫情及地缘政治因素的影响，对网络安全的投资有所降低，因此，与上期预测相比，本次预测 IDC 下调了网络安全市场规模的增速。当然，中国网络安全市场增长的核心逻辑并没有变化，客户对于网络安全建设的需求仍在不断增加，待疫情影响修复，中国的网络安全市场仍将保持着高速增长。IDC 最新数据显示，到 2026 年，中国网络安全支出规模预计接近 288.6 亿美元，五年复合增长率将达到 18.8%，增速位列全球第一。



https://mp.weixin.qq.com/s/s6CG1zM_KJd6F0vh0TOjbw

4、使用神经网络，NIST 抗量子算法第四次被破解

近日，瑞典皇家理工学院研究团队发表论文，称其提出一种新的神经网络训练方法“递归学习”(Recursive Learning)，并通过周期性循环旋转信息，实现了对美国国家技术标准研究院(NIST)四种抗量子密码安全算法之一 Crystals - Kyber 最高 5 阶掩码的侧信道攻击，以高于 99%的概率从中恢复了信息位(message bit)。

Crystals - Kyber 已被 NIST 选为待标准化的公钥加密和密钥封装机制，同时也被纳入美国国家安全局(NSA)推荐用于国家安全系统的密码算法套件，这使得评估 Crystals -

Kyber 对侧信道攻击的抵抗能力变得非常重要：侧信道攻击利用从物理可测量的非主信道获得的信息，例如运行实现的设备的时序或功耗。

https://www.secrss.com/articles/52211

5、苏州市数据出境安全评估申报备案平台上线

为保障数据要素安全跨境流动，服务苏州数字经济发展，依据《数据出境安全评估办法》和《江苏省数据出境安全评估申报工作指引（第一版）》，苏州市委网信办在“苏商通”门户网站、移动端 APP 推出苏州市数据出境安全评估申报备案平台，为企业“一站式”申报数据出境安全评估开通便捷通道，提供工作指引、申报备案、异议申报、申报咨询、政策动态五类服务。

https://mp.weixin.qq.com/s/ZjHf0wdqrpGahje7JuA_UA

业界观点

1、范泷渤：数字经济时代，防“数据泄露”仍是数据安全首要目标

数字化时代，数据赋能千行百业，数据泄露问题也随之而来。据 Proxyrack 给出的数据统计，中国在数据泄露数量 Top10 国家中位列第三，共被 Proxyrack 统计到 51309972 起数据泄露事件。

数据一旦泄露，是所有利益相关方的巨大损失，面对数据泄露问题，企事业单位有必要形成一套切实有效的数据防泄露管控系统，才能更好地应对和处置此类事件的发生：

在管控之前，要对所涉及到的敏感数据进行识别，比如结合先进的文档指纹匹配、数据库指纹匹配、精确数据匹配、图片指纹匹配、文件特征匹配、自然语义分析、机器学习等智能算法，准确识别出终端上的敏感数据、重要数据及数据安全风险行为。

在管控过程中，通过数据发现扫描和文件分级分类，形成重要数据分布地图，为运维人员梳理出清晰的数据分布情况，做到对终端上持续变化的数据存储进行监控，更好地减轻运维人员对于敏感信息难发现、难处置的实际问题。

数据防泄露系统通过对不同数据通道、不同等级、不同

严重性、不同内容的数据进行差异化响应控制（审计、提醒、询问、阻止、上传文件），从而实现既可以对重要、敏感数据进行保护，对潜在的数据泄露行为进行震慑并阻止敏感数据外泄，又可以不影响员工日常办公的目标。

https://www.secrss.com/articles/52202

2、解读丨王鹏：从布局规划看未来数字中国建设

近日，中共中央、国务院印发了《数字中国建设整体布局规划》。《规划》强调坚持以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导，提出2025年基本形成横向打通、纵向贯通、协调有力的一体化推进格局的主要任务，明确数字中国建设“2522”整体布局框架。

一、数字中国建设整体布局规划的主要内容

第一，明确了未来数字中国建设目标。

第二，明确了未来数字中国建设的重点工作任务。

第三，加强整体谋划、统筹推进，加快数字中国建设。

二、数字中国建设整体布局规划的重要意义

建设数字中国是数字时代推进中国式现代化的重要引擎，是构筑国家竞争新优势的有力支撑。加快数字中国建设，对全面建设社会主义现代化国家、全面推进中华民族伟大复

兴具有重要意义和深远影响。

第一，有助于加速经济社会数字化转型。

第二，有助于推动经济社会高质量发展。

第三，为数据经济发展奠定基础，具有重要现实意义。

三、数字中国建设整体布局规划的亮点

第一，明确了有关数据要素的全方位管理体系和管理制度。

第二，明确了强化数字研发关键能力的方案。

第三，明确了领导干部的考核评价体系。

http://www.cbdio.com/BigData/2023-03/02/content_6172108.htm

3、盘和林：做强做优做大数字经济，“两化”是核心

近日，中共中央、国务院印发了《数字中国建设整体布局规划》，并发出通知，要求各地区各部门结合实际认真贯彻落实。《规划》指出，要全面赋能经济社会发展，做强做优做大数字经济。

从《规划》我们可以看到，数字产业化和产业数字化（“两化”）仍旧是我国数字经济发展的核心内容，数字产业化为产业数字化开启了新征程，为应对消费、生活、工作多样化和个性化需求，开启了数字产业化，而产业数字化，又反过来

促进数字产业的转型和升级，比如实体经济转型升级遇到的数字技术、数字设备、数字零件的难题，又需要数字产业的突破、创新和支持。

数字经济“两化”经过几年的发展，虽然相辅相成，相互促进，但也呈现出了相互独立的趋势，具体而言，数字产业化聚焦需求端，产业数字化聚焦供给端，数字产业化以数据信息为核心，产业数字化以实体经济为核心，除此之外，两者涉及的产业规模和产业范围也不尽相同。

我国不论是产业数字化方面，还是数字产业方面，都存在着巨大的发展进步空间，第三轮信息技术革命下，全球竞争格局重新洗牌，产业链重构，产业逆向回流，保证本国产业链的安全和稳定是各国经济发展的重点。

因此，务必做强做优做大数字经济。首先，**加强数字基建建设**，数字基建是产业数字化和数字产业化发展的重要根基，可以看到，《规划》指出，要夯实数字中国建设基础。要立足于我国产业数字化和数字产业化发展的现状，加大对数字基建的投入，加快数据中心、东数西算、5G 网络与千兆光网等数字工程的建设，提升我国数据处理能力，实现数字产业和实体产业的高效发展。其次，**要强化数字平台和数字人才的力量**，一方面，通过学历教育和职业培训，培育专业的数字化人才，为产业的健康可持续发展提供保障，形成自立

自强的创新体系，另一方面，数字平台的建设，对于链接平台、服务商、商家、消费者，建立四方协同的价值共创模式，不仅降低了商家数字化转型的门槛和成本，为企业数字化转型提供方案，更增加了商家的利润，带动了消费的增长。最后，要**加大产业链数字化建设力度**，实现数字基础设施的高效联通，数字产业和实体产业价值的高效释放，以及资源的有效利用，数字经济发展质量效益的大幅增强，这样才能更好地完善数字治理体系，提升数字安全保障能力。

http://www.cbdio.com/BigData/2023-03/03/content_6172119.htm

4、邵志清：我国亟待建立多层次数据要素市场

“数据要素市场已经成为国家竞争优势的重要内容。”全国政协委员、致公党上海市委专职副主委邵志清表示。

经过多年实践，我国明确了数据要素市场的基本形态，以政府支持建设的数据交易机构为枢纽，促进数据流通交易，打造全链数商生态，推动数据资产化进程。不过，在邵志清看来，我国数据要素市场还处于发展初期，还存在一些主要问题：

第一，数据交易机构急需全国层面的统筹规划，难以发挥全国统一大市场的联动和规模效应。

第二，建设资源有待集中，尚无数据交易机构建成相对完善的数据流通交易基础设施。

第三，基础设施和市场发展有待提速，数据资产化尚处于理论验证到试点落地的过渡阶段。

针对上述问题，邵志清建议我国应**制定加快培育全国统一数据要素市场体系的指导意见**。建立分工明确、协同推进的多层次数据要素市场建设工作机制，避免各部门、各地方重复建设。明确多层次数据要素市场的总体架构和具体目标，加快建设国家数据交易所、有序推进地方数据交易中心建设、积极推动行业数据交易中心建设、引导多层次数据交易市场联动发展。完善统一数据要素市场功能，建立数据要素流通交易制度和标准体系，加强数据要素交易市场基础设施建设，加强组织保障。

同时，**需要集中资源，重点支持建设国家数据交易所**。支持上海、北京、深圳等条件成熟的地区建设国家数据交易所，按照“确立合法身份”和“落实法定功能”的发展阶段，完善法律、标准、政策和财政工具包。支持国家数据交易所开展数据要素基础制度创新试点，加快建设服务全国的数据基础设施，开展数据产品交易、数据资产登记、数据资产凭证管理等服务，有效链接地方和行业数据交易中心，打造全国统一数据要素市场的功能枢纽。依托国家数据交易所建设数

据要素流通国家工程研究中心，加强相关理论问题与技术规范的研究。

此外，邵志清还建议，**加快推进数据资产化，赋能多层次数据要素市场高质量发展**。按照登记确权、资产入表、资产应用三步走的路径推进数据资产化。建立全国统一的数据资产市场，明确国家数据交易所为数据资产登记确权机构，进行全国统一的数据资产登记和公告，赋予登记主体数据资源持有权和数据产品经营权，建立权益保护和权利流转机制。明确数据资产凭证管理机构，创新以数据产品交易凭证为纽带的数据资产价值认定和动态估值机制，依托国家数据交易所打造一批数据资产入表示范企业。在数据资产登记确权、资产入表的基础上，探索数据资产作价入股、抵押融资、资产证券化等更为广阔的资产应用。

值得一提的是，支撑数据要素有效流通的信息基础设施至关重要，对此，邵志清认为，应支持重点地区“云、链、网、技”建设，**尽快打造多层次数据要素市场的基础设施**，为场内集中交易和场外分散交易提供低成本、高效率、可信赖的流通环境。提升基础设施的效率能力，实现业务流程自动化和智能化，提高匹配效率和业务处理效率。通过应用区块链和可信隐私计算技术，搭建互通互联的交易系统和可信可控的交易环境，从而提升基础设施的合规能力。

http://www.cena.com.cn/industrynews/20230304/119224.html

5、周汉民：建立政府使用个人信息数据公开制度

近年来，我国陆续出台了相关法律，为守卫个人信息提供了法治保障，但在实践应用中，仍存在术语界定模糊、权属不清、监管滞后等短板。对此，全国政协委员、上海市社会主义学院院长、上海中华职教社主任周汉民，在提交全国政协十四届一次会议的提案中，建议进一步完善相关配套措施，优化细节，如建议建立政府使用个人信息数据公开制度，加大对违法行为的惩处力度，让个人信息保护法律真正落地生根。

周汉民委员认为，从个人信息保护的立法来看，目前主要存在以下问题:术语界定模糊。“另外,个人信息权属不清，目前尚无法律对个人信息的权属作出统一规定。同时，监管滞后，增加了个人信息与隐私泄露的风险。”

针对这些问题，周汉民委员提出了几条解决建议:

发布个人信息保护民商事指导性案例，由最高人民法院组织发布个人信息保护民商事指导性案例，分别发布有关个人信息概念界定方式、权属确认方法、个人信息保护底线等方面的指导性案例，为法官统一裁判标准、统一认定方法提供指引。在出台指导性案例后，最高法出台《个人信息保护

法》司法解释，为此后修订完善《网络安全法》《个人信息保护法》以及衔接《民法典》提供参考。

建立政府使用个人信息数据公开制度，出台“政府使用个人信息数据公开目录”，尤其在有关个人信息类型、数据要素市场以及使用方式等公开环节广泛听取社会公众意见，将公众对数据类型的需求强度纳入评判是否应使用个人信息乃至是否可进行交易流通的参考指标。另一方面，进一步加强个人信息流通的监管。

加大对违法行为的惩处力度，建立公民电子信息投诉制度，具体包括受理范围、处理流程以及投诉反馈制度。对保护公民个人电子信息确有过错的，按照过错程度责令整改和进行相应处罚，以企业为例，可考虑暂扣相关行政许可执照，以企业年、半年或季度营业收入的一定百分比分别罚款。若情节特别严重，应当移送有关部门，撤销营业所需行政许可。https://finance.sina.com.cn/jjxw/2023-03-04/doc-imyismae1383825.shtml

数据安全事件

1、美国法警局遭遇重大安全事件，涉及敏感信息泄露

3 月 2 日报道，美国法警局 (USMS) 宣布勒索软件攻击影响了“独立的 USMS 系统”。目前正在调查安全漏洞后敏感信息被盗的情况。作为司法部内的联邦执法机构，USMS 通过追捕逃犯、保护政府证人及其家人、执行联邦法院命令等来支持联邦司法系统。

据称，除了有关 USMS 调查的敏感信息外，受感染的系统还包含个人身份信息。“受影响的系统包含执法敏感信息，包括法律程序的返回、行政信息以及与 USMS 调查对象、第三方和某些 USMS 员工有关的个人身份信息，”发言人说。

USMS 发现数据从受影响的系统中泄露，将此次攻击视为重大事件，但表示它已经能够继续运营。

https://mp.weixin.qq.com/s/E7h8Pv-oQo9a-wSmEp3Fww

2、软件巨头 Beeline 数据库在暗网公布，亚马逊、波音、摩根大通等都受影响

2 月 28 日报道，美国软件公司 Beeline 的数据库被攻击者发布在黑客论坛上，数据库内包含亚马逊、瑞士信贷、3M、波音、宝马、戴姆勒、摩根大通、麦当劳、蒙特利尔银行等

Beeline 客户的数据。

该数据库大约 1.5GB，据称是攻击者从 Beeline 的 Jira 账户中窃取的。Jira 是由 Atlassian 开发的问题跟踪软件，用于 bug 跟踪和项目管理活动。与此同时，Beeline 运营着一项软件即服务（SaaS）业务，专注于寻找和管理劳动力。

攻击者声称该数据库包含 Beeline 的客户数据，例如名字、姓氏、Beeline 用户名、职位以及其他数据。

https://mp.weixin.qq.com/s/Y5tY44NXGNo6ocFmL_YZgg

3、在 GoAnywhere MFT 遭黑客入侵后，Hatch Bank 披露了数据泄露事件

3 月 2 日报道，在黑客从该公司的 Fortra GoAnywhere MFT 安全文件共享平台窃取近 140,000 名客户的个人信息后，金融科技银行平台 Hatch Bank 报告了数据泄露事件。

TechCrunch 报道，根据该公司发送给受影响客户并提交给总检察长办公室的数据泄露通知报告称，黑客利用 GoAnywhere MFT 软件中的漏洞窃取了 139,493 名客户的数据。Hatch 表示，他们对被盗数据进行了审查，并确定客户的姓名和社会安全号码被攻击者盗用。

虽然 Hatch Bank 没有透露是哪个威胁者发起了这次攻击，但 Clop 勒索软件团伙声称他们是这些攻击的幕后黑手

https://www.bleepingcomputer.com/news/security/hatch-bank-discloses-data-breach-after-goanywhere-mft-hack/?&web_view=true

4、LastPass 用户数据遭窃：关键运维员工遭定向攻击，内部安全控制失效

3 月 2 日消息，密码管理供应商 LastPass 日前公布了去年遭受“二次协同攻击”事件的更多信息，发现恶意黑客潜伏在其内网长达两个月的时间内，持续访问并窃取了亚马逊 AWS 云存储中的数据。

“二次协同攻击”事件，是指 LastPass 在 2022 年 8 月、12 月先后披露的两起违规事件，这两起事件的攻击链有关联。

LastPass 称恶意黑客使用到了去年 8 月首次入侵时窃取的信息，还利用一个远程代码执行漏洞，在一名高级 DevOps 工程师的计算机上安装了键盘记录器。由于恶意黑客窃取并使用了有效的访问凭证，LastPass 的调查人员很难检测到对方活动，导致其顺利从 LastPass 的云存储服务器处访问并窃取到大量数据。

https://www.secrss.com/articles/52411

5、视频营销软件 Animker 泄露大量用户数据

3 月 1 日，据外媒报道，一个配置错误的数据库暴露了属于 getshow.io(一体化视频营销平台)和 animaker.com(DIY 视频动画软件)网站的超过 700,000 名用户的测试和个人数据。

该数据库目前包含 5.3 GB 的数据，并且随着每天添加新数据而不断增长。因错误配置而泄露的数据包括：客户全名、设备类型、IP 地址、手机号码、邮件地址、Animaker 个人资料详情等。任何人都可以访问该服务器，无需绕过安全验证即可访问和下载数据。

https://www.hackread.com/video-marketing-software-animker-data-leak/?web_view=true

6、BidenCash 市场在周年活动中泄露了 200 万张信用卡信息

3 月 2 日，据外媒报道，BidenCash 是一个臭名昭著的暗网信用卡市场，向公众提供被盗的信用卡详细信息。作为其生日周年促销活动的一部分，已经泄露了超过 200 万张有效信用卡，泄露的数据集包含来自世界各地的银行卡信息，其中有相当一部分是在美国、中国、墨西哥、印度、加拿大和英国发行的。

泄露的信息包括持卡人的全名、卡号、银行详细信息、有效期、卡验证值 (CVV) 号码、家庭住址和超过 500,000 个电子邮件地址。

https://www.hackread.com/bidencash-leaks-2-million-credit-cards/?web_view=true

7、加拿大图书巨头称员工数据在勒索软件攻击中被盗

3 月 1 日，据外媒报道，加拿大书商 Indigo 上个月遭受了一起勒索软件攻击事件，导致其网站瘫痪。近日，其表示员工数据在攻击中被盗。

Indigo 在加拿大各地的 160 多家商店拥有 8,000 多名现有员工。“通过调查，我们了解到没有理由相信客户数据被不当访问，但一些员工数据确实被盗。我们发出了泄露通知并正在与执法部门合作，”该公司表示道。

https://therecord.media/indigo-book-seller-employee-data-ransomware-attack/?web_view=true

8、涉疫个人数据开始销毁！无锡首批销毁 10 亿条

3 月 2 日晚，据无锡市公安局官微“平安无锡”消息，无锡市当日举行涉疫个人数据销毁仪式，首批销毁数据 10 亿

条。同时门铃码、疫查通、货运通行证等 40 多项“数字防疫”应用也于当天陆续下线。

无锡市城运中心数字底座部副部长王娟介绍，这部分数据主要集中存放在政务云平台，可以通过集中销毁数据存储介质的方式确保数据彻底销毁，无法恢复。为确保数据彻底销毁、无法还原，还邀请了第三方审计和公证处参与工作。

“此次销毁涉疫个人数据，一是体现了依法执政理念，依法依规删除目的已经实现的数据；二是保护了公民隐私，防止数字时代公民个人信息被盗用或滥用；三是防止了数据泄露，通过数据彻底销毁减少数据泄露的可能性；四是节约了存储空间，进一步提高存储效率。”无锡市大数据管理局副局长颜春水说。

https://mp.weixin.qq.com/s/2dHJaDGQoRWTKQyRWP5Ctw

9、美国和加拿大以“数据安全”为由禁止政府机构使用国际版抖音（TikTok）

当地时间 2 月 27 日，美国白宫管理和预算办公室主任 Shalanda Young 指出，除非有极少数例外情况，所有行政机构及其承包商必须在通知发布后的 30 天内删除 TikTok 或其母公司字节跳动的任何应用程序。机构必须在 90 天内在合

同中包括短视频应用程序不能在设备上使用，并取消任何需要该应用程序使用的合同。

美国拜登政府表示其对美国用户数据安全性产生了担忧，担心数据可能会传到中国政府手中。因此，美国官员以中国政府可能会向字节跳动施加压力，要求其提供从用户那里收集到的隐私信息，且这些信息可以用于情报或虚假信息目的为由持续打压 TikTok 应用及其母公司字节跳动。

此外，加拿大政府也宣布将从本周二开始禁止政府设备上的 TikTok 应用程序，欧洲委员会上周也发布了自己的禁令，禁止在官方设备上使用该应用程序，理由是出于网络安全方面的考虑。

https://mp.weixin.qq.com/s/xQYUcBpsK0_Q48QCuiDEzA

10、Play 勒索软件团伙已开始泄露从奥克兰市窃取的数据

3 月 5 日，据外媒报道，Play 勒索软件团伙在最近的一次网络攻击中开始泄露他们从奥克兰市（加利福尼亚州）窃取的数据。

奥克兰是旧金山湾区东湾区最大的城市，加州人口第八大城市。该市于 2023 年 2 月 10 日披露了一次勒索软件攻击，出于谨慎考虑，奥克兰市将受影响的系统下线，同时他们努力保护受影响的基础设施。

3 月 3 日，经证实，未经授权的第三方从其网络中获取了某些文件，并威胁要公开这些信息。声称对这次攻击负责的 Play 勒索软件组织开始泄露一个 10 GB 的档案，其中包含敏感数据，例如员工信息、护照和 ID。

https://securityaffairs.com/143037/cyber-crime/play-ransomware-leaks-city-of-oakland.html

11、黑客入侵枪支买卖网站 GunAction.com，窃取大量用户数据

3 月 3 日，据 TechCrunch 报道，一个黑客团伙成功入侵枪支买卖网站 GunAuction.com，窃取超过 55 万名用户的敏感个人数据（数据主要包括姓名、家庭地址、电子邮件地址、密码和电话号码等）。

TechCrunch 指出，GunAuction.com 数据泄露事件或产生严重后果，例如潜在犯罪分子通过被盗数据获悉用户的实际住址，直接潜入受害者家中，窃取武器。

https://www.freebuf.com/news/359264.html

12、英国零售连锁店 WH Smith 称数据在网络攻击中被盗

3 月 2 日，据外媒报道，英国零售商 WH Smith 遭遇数据泄露，暴露了属于现任和前任员工的信息。

WH Smith 在英国经营着 1,700 个商店，拥有超过 12,500 名员工。该公司表示，此次攻击并未影响其贸易业务。客户数据没有受到影响，因为该类型信息存储在单独的系统上，不会受到未经授权的访问，确认受事件影响的个人将直接收到通知。

https://www.bleepingcomputer.com/news/security/british-retail-chain-wh-smith-says-data-stolen-in-cyberattack/?&web_view=true

《全球数据安全观察》周报

政策形势： 政策法规/地方动态/标准动态

技术、产品与市场： 技术研究/行业洞察/市场趋势

业界观点： 大咖观点/业界报告

数据安全事件： 合规事件/数据泄露/数据勒索

编委会： 钟力、唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nelab@360.cn

http://www.nelab-bdst.org.cn/