全球数据安全观察

总第 130 期 2023 年第 11 期

(2023.03.20-2023.03.26)

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、《网信部门行政执法程序规定》发布，6 月 1 日起施行

3 月 23 日，国家互联网信息办公室公布《网信部门行政执法程序规定》（以下简称《规定》），自 2023 年 6 月 1 日起施行。相关负责人表示，出台《规定》，是为了进一步规范和保障网信部门依法履行职责，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益。《规定》规范了网信部门行政执法程序，明确了行政处罚执行，规定了行政处罚应接受社会监督。

http://politics.people.com.cn/n1/2023/0327/c1001-32651415.html

2、中共中央办公厅、国务院办公厅印发《关于进一步完善医疗卫生服务体系的意见》

新华社 3 月 23 日电，中共中央办公厅、国务院办公厅印发《关于进一步完善医疗卫生服务体系的意见》。意见提出，发展“互联网+医疗健康”，建设面向医疗领域的工业互联网平台，加快推进互联网、区块链、物联网、人工智能、云计算、大数据等在医疗卫生领域中的应用，加强健康医疗大数据共享交换与保障体系建设。建立跨部门、跨机构公共卫生

数据共享调度机制和智慧化预警多点触发机制。推进医疗联合体内信息系统统一运营和互联互通，加强数字化管理。加快健康医疗数据安全体系建设，强化数据安全监测和预警，提高医疗卫生机构数据安全防护能力，加强对重要信息的保护。

https://mp.weixin.qq.com/s/9CYi6JpRiUeHBs6cp5CGJw

3、郑州市人民政府印发《郑州市政务数据安全管理实施细则》

郑州市人民政府近日印发《郑州市政务数据安全管理实施细则》。《实施细则》要求**政务部门规范政务信息系统和政务数据资源管理，采取安全策略和技术措施**，加强对数据收集、存储、传输、共享、开放、使用、销毁等全生命周期的安全保护，并强调加强个人信息保护。要求**市政务数据主管部门会同网信、公安等部门建立应急协调机制**，政务部门应按照本级政务数据主管部门和上级业务主管部门要求，建立政务数据安全应急管理机制，及时进行应急处置。

https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20230316143506&norm_id=20221102152946&recode_id=50381

4、公布 8 起典型案例！公安机关依法严厉打击侵犯公民个人信息犯罪

近日，按照公安部统一部署，全国公安机关网安部门聚焦人民群众反映强烈的各类侵犯公民个人信息违法犯罪活动，依托“净网 2022”专项行动，坚持“追源头、打内鬼、端平台”，持续开展严厉打击侵犯公民个人信息犯罪工作，破获一批重大案件，抓获一批犯罪嫌疑人，取得明显成效，有力维护了网络空间安全和社会公共安全。公安部今日公布打击侵犯公民个人信息犯罪 8 起典型案例。

https://mp.weixin.qq.com/s/tRlDLFQdvI1yjYAN0YJHQA

5、《电信领域数据安全指南》等 12 项网络安全国家标准获批发布

根据 2023 年 3 月 17 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2023 年第 1 号），全国信息安全标准化技术委员会归口的 12 项网络安全国家标准正式发布，实施时间为 10 月 1 日，包括《电信领域数据安全指南》、《个人信息去标识化效果评估指南》、《网络安全从业人员能力基本要求》等。

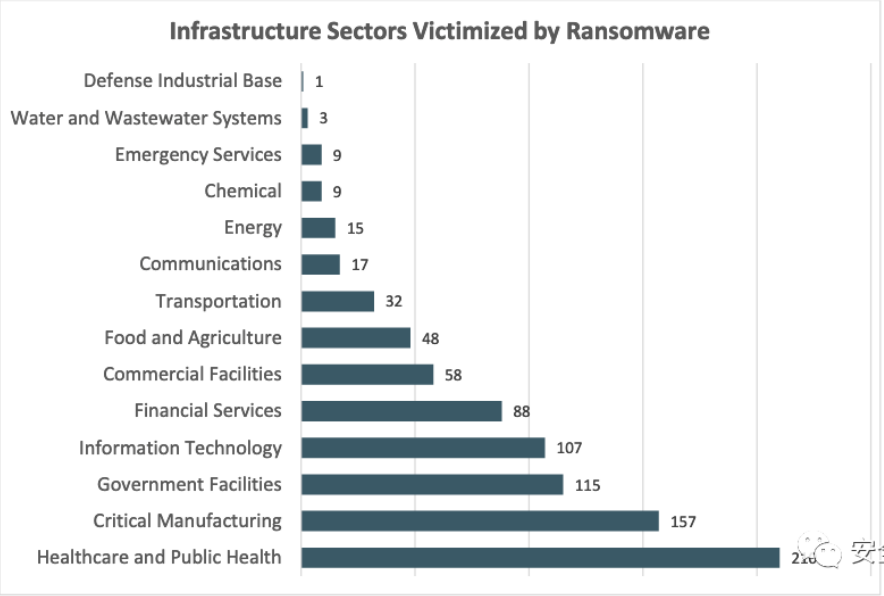
https://mp.weixin.qq.com/s/iVAf9aVaD0UeM0ci2uyvFA

技术、产品与市场

1、FBI：去年至少 860 个关键基础设施遭勒索软件入侵

3 月 22 日消息，美国联邦调查局（FBI）在 2022 年互联网犯罪报告中披露，**勒索软件团伙去年共破坏了至少 860 个关键基础设施组织的网络**。

整个 2022 年，勒索软件受害者共提交 2385 起投诉，综合损失超过 3430 万美元。**按攻击次数计算，去年关基攻击活动中最为活跃的三大勒索软件团伙分别是 Lockbit（149 起）、ALPHV/BlackCat（114 起）和 Hive（87 起）。**



https://www.secrss.com/articles/52998

2、IDC：2023 年中国网络安全支出增速超过美国

根据 IDC 最新发布的数据，2023 年，全球网络安全解决

方案和服务支出预计将达到 2190 亿美元，较 2021 年增长 12.1%，中国网络安全市场增速超过美国，但美国依然是 2023 年全球最大的网络安全地区市场。

端点安全成最大投资热点：2023 年在安全产品和服务方面支出最多的行业是银行、离散制造、专业服务和联邦/中央政府。银行和离散制造企业在安全软件和服务上的投入规模持平，其中最大的支出用于托管安全服务。相比之下，安全专业服务的软件方面将获得更多投资，重点是治理、风险和合规性（GRC）以及端点安全。安全服务支出也将是联邦/中央政府最关注的领域。到 2023 年，银行、离散制造、专业服务和政府这四个行业加起来将占所有安全支出的三分之一以上。IDC 预测，2021-2026 年网络安全支出增长最快的行业是证券和投资服务、电信和银行。软件将成为 2023 年最主要的网络安全支出，占全年所有安全支出的近一半。**其中最热门的投资是端点安全，其次是身份和数字信任软件、网络安全分析、威胁情报、响应和编排软件。**

https://www.secrss.com/articles/52954

3、《数据安全管控平台应用指南》报告发布

在近日召开的 2023 数据安全技术创新和管理认证研讨会中，安全牛联合多家国内数据安全技术代表性厂商，共同

发布《数据安全管控平台应用指南》报告，旨在更好满足我国企业对新一代数据安全管控技术的应用需求，探索数据安全体系化能力建设的成功经验。报告关键发现如下:

（1）数据安全管控平台不仅是实现多种数据安全工具的统一配置管理，而是要能够帮助企业实现数据全生命周期的监控与防护，需要具备统一的安全分析能力、策略配置能力、威胁发现能力、协同处置能力和运营管理能力;

（2）数据安全管控平台产品已成为各大数据安全厂商技术研发的重点，但由于目前甲方侧的应用多处于验证测试或建设部署阶段，方案成熟度有待实际验证，方案实际可用性仍需要进一步提升;

（3）数据安全管控平台不仅是企业新一代数据安全管理体系构建的核心要素，也是企业有效开展数据安全治理的重要支撑能力;

（4）在数据安全管控平台的实际建设与应用中，会面临业务场景复杂、定制化需求高、产品认知不足、持续运营能力缺乏、工具协同难度大、组织管理职责不明等挑战;

（5）数据安全管控平台将在元数据分析、非结构化数据防护、数据攻击面管理等方面进行能力优化和完善。

https://mp.weixin.qq.com/s/nw2-hMci_eJAmaZ0QniFqw

4、《数据安全管理认证建设指引》白皮书发布

企业组织不仅需要构建全面的数据安全管控体系，同时还需要根据国家主管部门的要求，尽快开展数据安全管理的认证工作，以促进数据安全管理体系健全与优化。通过《数据安全管理认证建设指引》白皮书的编制，旨在为企业未来的数据安全工作提供更多方法论支持。

报告研究分析《数据安全管理认证实施规则》，明确认证范围、流程、模式等，为甲方用户提供通过认证的指导；围绕《数据安全管理认证》所依据的《GBT 41479-2022 信息安全技术网络数据处理安全要求》，开展数据安全治理体系建设研究。

https://mp.weixin.qq.com/s/a5r3oJaS6DAx980nOdFYrA

5、IDC MarketShare：中国数据泄露防护市场份额，2022 报告研究正式启动

数据泄露防护（DLP）作为数据安全方向成熟度较高的主导性技术正倍受关注。为了更直观的展现 2022 年的中国数据泄露防护（DLP）产品市场，IDC 正式启动 2022 年中国数据泄露防护市场的深入调研。

IDC 定义下的数据泄露防护技术包括广泛的解决方案，实现对存储和使用过程中的敏感信息的发现、监测和保护，

从而检测和防护对敏感信息的未授权访问和传输。数据泄露防护包括两种实现方式:

（1)终端数据泄露防护: 在台式机、笔记本、移动设备、USB 驱动、文档/存储服务器，以及其它类型的数据资源库上执行强制策略，防止敏感数据泄露。

（2）网络数据泄露防护：对邮件、即时通讯、FTP、基于 Web 的工具（例如 HTTP 或者 HTTPS），以及点对点应用执行策略，组织敏感数据的泄露。

https://mp.weixin.qq.com/s/0bH8DLPYTYupywWJzF2UfQ

业界观点

1、人民财评：打破壁垒，让数据潜能得到充分释放

在今年两会上，数据流通问题受到代表委员关注，“在数据流通层面，存在‘有数据的单位不愿开放、有需要的单位拿不到数据’现象，数据资源的开放共享有待加强。”针对这种情况，有代表建议，推进数据要素交换平台的市场化运营，提升数据要素流通技术能力，让数据潜能得到充分释放。

充分发挥数据潜能，需要进一步完善制度建设。今天，信息化已经渗透到社会生活的方方面面，人们日常生产生活中，每时每刻都在产生大量的数据。这些数据看不见摸不着，却真实存在。然而，这些数据归谁所有、谁有权利用、使用范围如何界定、使用安全如何保障、个人和企业如何保障自己的数据不被滥用等等，一系列问题都有待厘清。信息化时代，新产业、新技术、新业态、新商业模式不断更新迭代，如何在鼓励创新发展的同时，规范其在数据方面的应用，同样需要研究探索。

充分发挥数据潜能，需要进一步加强产业化建设。数据本身不能产生价值，它只是保存在不同存储介质上的无数个0和1。只有对其进行科学地收集、整理、分析、验证，才能从中得出正确的规律和有价值的信息，从而为社会发展提供

助力。而在这一过程中，需要打破数据的割裂状态，让不同渠道的数据能充分共享，通过海量数据的交叉比对，更有效地发挥其潜能。在这方面，目前还存在一些障碍。很多部门和企业因职能原因，汇聚了大量数据，而另外一些部门和企业则有对这些数据的强烈需求。但是目前，拥有数据的部门和企业，在数据共享方面，既没有法律支持也缺乏主观意愿。归根结底，是由于目前我国尚未形成数据要素流转市场的基础制度，数据流通利用面临产权归属不明、定价机制不清、交易信任机制不畅等问题。因此，加强市场建设，逐步打造全国层面多层次数据要素市场的统筹布局，需要有关部门尽快加以规划推进。

充分发挥数据潜能，同样不能忽视数据安全。公共数据体量巨大、价值含量高，对于社会治理和产业发展，都蕴藏着巨大的价值。在打造数据要素流转市场的过程中，保障数据安全，防止数据被滥用和泄露，必须予以高度重视。

http://opinion.people.com.cn/n1/2023/0319/c427456-32646909.html

2、张云泉委员：夯实数据基础设施 促进上云数据流动和安全

我国近年来在不断推进企业数字化转型，陆续发布了

《关于推进“上云用数赋智”行动 培育新经济发展实施方案》、《关于加快推进国有企业数字化转型工作的通知》等政策文件，均鼓励企业“上云用数赋智”。

目前上云企业累计超过380万家，超过70%的企业使用了多个云，存储在云上的数据量超过传统数据中心，上云用数赋智已经成为企业数字化转型的重要方向和发挥数据要素价值的重要基础。但企业在上云过程中面临着数据流动和数据存储上的诸多问题。这体现在几个方面。

一是数据基础设施的建设方式落后，数据难以流动。数据流动往往发生在多个云之间，在我国，由于云平台提供商绑定使用自己的数据存储设备，企业每建设一个云就对应一套独立的数据存储设备，在事实上形成了多个云数据孤岛，数据难以共享和流动。

二是数据存储存在安全风险。75%的云上数据都存储在机械硬盘中，机械硬盘的产业链高度集中，100%被垄断在美国希捷、美国西部数据、日本东芝三家厂商手里，导致使用机械硬盘的产品更容易被植入“后门”、存储信息更容易被窃取、存储服务器设备更容易被攻击破坏。由于缺少整体替代规划，闪存在国内数据存储中的普及率还非常低，据Gartner/IDC 统计，美国闪存占比 56.4%，全球平均 41.3%，在中国闪存占比不到15%。

三是数据存储效率低，无法满足低碳发展。按现有架构继续发展，预计2025年数据存储的耗电量将达到630亿Kwh，耗电量占全国用电量比重0.91%。

基于此，张云泉提出几方面建议。

首先是鼓励数据基础设施的建设方式升级。在推进企业上云用数赋智的相关规划中，制定云平台和数据存储的互联互通标准，鼓励企业建设统一的数据存储资源池。

其次是加快闪存数据存储的应用节奏。制定针对国外机械硬盘存储设备的国产闪存产品替代工作方案和时间表，并将其纳入企业数字化转型工作计划。

最后，加大对新型存储架构的科研创新资金投入和产业扶持力度。将新型存储架构创新作为重点支出事项和战略投入重点，设立专项资金，引导龙头企业联合高校、科研院所，将基础研究、技术创新、产业创新与市场应用有机结合。打造一批以新型存储架构应用为代表的示范区、示范基地，通过政策支持加速相关技术产品产业化和应用。

https://news.sciencenet.cn/htmlnews/2023/3/495316.shtm

3、邵志清委员：建议加快建设国家数字信任平台

新型数字信任体系是一个国家可持续发展和数字化转型成功的重要影响因素，要加快建设国家数字信任平台。目

前，实现数据安全合规可信的流通，存在三方面主要问题亟待解决：一是数据安全事件频发，公众对企业和机构数据保护能力的信心不足。二是网络信任体系中身份的互操作和监管问题。三是数据可信流通制度体系和技术体系有效协同的问题。

对此，邵志清建议，要结合数据要素市场化配置，对数字信任基础设施进行顶层规划。“应该将数字信任的构建纳入数字政府治理的范畴，制定中国数字信任体系的远景、目标、领域、指导原则、责任模型和关键能力等。同时，统筹规划数字信任制度体系和技术体系，建立数据安全、权利保护、跨境传输管理、交易流通、开放、共享、安全认证等基础制度和标准规范，建立统一、规范的数字身份和数据安全合规监管体系，并且要积极鼓励试验探索，参与国际标准规范制定。”

如何加速数据共享流通信任体系建设？邵志清还建议，强化数据安全合规监管能力，统一拟定数据安全标准规范，引导数据要素市场参与者基于统一的规则按需建设数据安全防护和管理能力。加强数据安全和隐私保护能力的集约化供给，推动身份认证、网络安全、数据安全、密码、隐私计算等能力的公共服务化。加快构建数据流通监管体系，建立数据要素确权，存证等规则体系，运用密码学和区块链等技

术实现穿透式、全方位的监管。

https://www.chinanews.com.cn/gn/2023/03-02/9963999.shtml

4、我国数据安全法的体系逻辑与实施优化

我国《数据安全法》采取综合立法模式，形成我国对数据安全的原创性制度实践。《数据安全法》拓展了传统数据安全的含义，其立法逻辑隐含了“安全—控制—利用”三个层次，以适应数据开发和利用所伴随的安全风险加剧的现实。从域外经验来看，美欧等数字经济发达国家或地区近年来通过多个单行立法的形式，同样沿着“安全—控制—利用”的三层结构，构建了各自独特的数据战略。相比之下，目前的《数据安全法》的实施和落地，无论在战略层面和具体制度构建层面都存在不足，应当对此予以针对性优化。

从安全的层次看，《数据安全法》对于数据流转中的安全风险制度设计提出了原则性的要求，但对数据流动过程中的安全风险并没有提出针对性的措施。数据流转中的安全如何保障，是数据安全立法需要专门设计的内容，《数据安全法》的实施应进一步考虑保障数据流动链条中所有参与主体较为一致的安全保障水平，并明确数据流动链条中上下游参与各方的安全责任划分问题。

从控制层面来看，《数据安全法》考虑到数据泄露的初始

风险乃至数据被不当分析利用可能造成的风险，而在传统国家秘密之外，提出了重要数据保护的基本框架。

从利用层面来看，目前《数据安全法》中关于利用的内容主要是关于政务数据安全与开放、公安机关和国家安全机关因依法维护国家安全或者侦查犯罪的需要而调取数据的规定，以及封阻来自于域外的调取数据要求，但相应内容大量使用了“依照法律、行政法规规定”“按照国家有关规定”等措辞，将相应的制度规范要求指向数据安全法之外的其他法律、行政法规，但又没有交代清楚具体依照哪部法律、行政法规的规定，有违法律规范应当明确、具体的特性要求。

https://www.secrss.com/articles/53090

5、AIGC 爆火之后：如何平衡数据流动共享与安全保护？

AIGC（人工智能生成内容）正在给人类社会带来一场深刻的变革。ChatGPT 等 AI 技术在数据收集、处理、输出等各环节都可能存在伴生风险，如未经授权收集信息、提供虚假信息、侵害个人隐私等等。监管方和相关企业亟需从制度和技术方面共同发力，加强 AIGC 领域数据安全保护。

吴沈括在接受 21 世纪经济报道记者采访时表示，ChatGPT 作为大语言模型，**它的核心逻辑事实上是海量数据的收集、加工、处理和运算结果的输出**。“总的来说，这几个

环节可能会在技术要素、组织管理、数字内容三个方面伴生相关风险。”

北京航空航天大学法学院副教授赵精武分析，在数据安全和个人信息保护领域，**ChatGPT 等 AI 技术的风险主要表现为用户输入的数据存在泄露风险**，倘若用户为了完成工作任务，输入了敏感个人信息、商业秘密等信息，这些信息有可能被 AI 服务提供者留存。如果国内企业试图引入 ChatGPT 服务，其合规要点在于：**一是输入输出数据应当留存于境内；二是需要经由工信部等主管部门审核，获得相应的信息服务资质认证；三是若对用户个人信息权益产生实质性影响，需要进行个人信息安全影响评估；四是如果国内企业属于关键信息基础设施运营者，其引入 ChatGPT 服务还需要进行网络安全审查。**

面对前述潜藏风险，监管方和相关企业如何从制度和技术层面加强 AIGC 领域的数据安全保护？

吴沈括建议监管侧关注三方面规则。“一是市场的准入和资质规则，确保优良主体进入该市场领域。二是业务监管规则，确保主体的运行符合既定的监管框架要求。三是责任规则，要划定行为红线、责任红线，明确各方主体的责任范围，规范市场秩序。”

赵精武认为，“相较于直接针对用户终端采取限制使用等

监管措施，明确要求 AI 技术研发企业遵循科技伦理原则会更具成效，因为这些企业能够在技术层面限定用户的使用范围。”

https://www.secrss.com/articles/52975

数据安全事件

1、麦当劳因泄露 487 万顾客的数据被韩国罚款 6.96 亿韩元

据媒体 3 月 22 日报道，麦当劳韩国公司因数据管理不严导致 487 万顾客的个人数据泄露，被罚款 6.96 亿韩元（约合 532110 美元）。根据调查结果，麦当劳没有进行充分的访问控制，使得包含其餐厅和麦当劳客户的个人数据的备份文件可以通过文件共享协议进行访问。结果，黑客入侵并泄露了超过 487 万客户的个人数据。此外，该公司还被发现没有销毁数据保留期已过的 766846 名顾客的数据，并且迟迟没有向当局和顾客通报数据泄露的情况。

https://en.yna.co.kr/view/AEN20230322007100315

2、全国首例全链条打击“非法获取公民车辆位置信息”案宣判

3 月 24 日，全国首例全链条打击“非法获取公民车辆位置信息”案，在南京市鼓楼区人民法院公开开庭审理并当庭宣判。

2020 年 6 月起，被告人黄某伦、李某两人，明知他人从事非法寻车业务，仍制作、提供“JTC”等程序并从中牟利。非法寻车业务经营者利用两名被告提供的“JTC”等程序，可

绕过某些停车平台系统的安全防护机制，非法获取车辆停车位置信息，或者根据客户需求在车辆底部等位置安装 GPS 设备，非法跟踪车辆行踪轨迹。

南京市鼓楼区人民法院认为，停车信息及车辆行踪轨迹，反映特定自然人的生活、工作等活动情况，属于公民个人信息，应受法律保护。两名被告人的行为已构成侵犯公民个人信息罪。

https://mp.weixin.qq.com/s/ZCTqecmpL0lMPFYzDFehuw

3、法拉利遭到勒索攻击导致部分客户的详细信息泄露

据媒体 3 月 20 日报道，意大利跑车制造商法拉利遭到勒索攻击。该公司称攻击者获得了其部分 IT 系统的访问权限，客户姓名、地址和电话号码等信息泄露。法拉利表示已采取措施保护受影响系统，且此次攻击对公司的运营没有影响。该公司没有说明攻击发生的时间，但这可能与 2022 年 10 月报道的勒索攻击有关，当时 RansomEXX 声称窃取了法拉利的 7 GB 数据。据消息人士称，最初的赎金要求是 100 万美元。法拉利在 3 月 20 日的声明中表示，不会付赎金。

https://www.securityweek.com/ferrari-says-ransomware-attack-exposed-customer-data/

4、荷兰航运公司 Royal Dirkzwager 遭到 Play 的勒索攻击

据 3 月 20 日报道，荷兰航运公司 Royal Dirkzwager 遭到勒索团伙 Play 的攻击。勒索团伙将该公司添加到其网站上，并宣布窃取了员工 ID、护照和合同等机密数据。该团伙最初公开了一个 5 GB 的文件作为攻击证据，并威胁说，如果公司不付赎金就公开全部的数据。该航运公司表示，攻击活动并未影响公司的运营，并证实攻击者已经从其基础设施中窃取了敏感数据。该公司已将此事通知了荷兰数据保护局，并正在与勒索团伙进行谈判。

https://securityaffairs.com/143714/cyber-crime/play-ransomware-royal-dirkzwager.html

5、LockBit 勒索软件团伙声称要泄露从奥克兰市系统中窃取的文件

3 月 21 日，据外媒报道，勒索软件活动 LockBit 团伙现在威胁要泄露它所描述的从奥克兰市系统中窃取的文件。然而，该团伙尚未公布任何证据证明他们从西海岸港口城市的网络中窃取了任何文件。

在 LockBit 暗网数据泄露网站的新条目上，他们警告说，他们拥有的所有奥克兰市数据将在 19 天内，即 4 月 10 日公布。奥克兰市尚未就 LockBit 勒索软件团伙的指控发表

声明。

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-now-also-claims-city-of-oakland-breach/?&web_view=true

6、流媒体平台 Lionsgate 近 3000 万条记录泄露

据 Cybernews 在 3 月 22 日报道，拥有 3700 万订户的视频流媒体平台 Lionsgate Play 的 ElasticSearch 配置错误，泄露了用户数据。研究人员发现了一个 20 GB 服务器日志，包含近 3000 万条条目，最早的日期是 2022 年 5 月。日志泄露了订阅者的 IP 地址以及有关设备、操作系统和 Web 浏览器的用户信息。还泄露了平台的使用数据，如用户观看内容的标题 ID 和搜索查询等，通常可用于分析和性能跟踪。Cybernews 就此事联系了 Lionsgate，该公司的回应是已将服务器保护起来，但是截至目前尚未提供官方回应。

https://cybernews.com/security/lionsgate-data-leak/

7、韩国美容平台近百万用户数据泄露

3 月 23 日，韩国社交平台 powderroom.co.kr（自称是该国最大的美容社区）泄露了一百万用户的私人数据。该平台公开了全名，电话号码，电子邮件，Instagram 用户名，甚至

家庭住址。研究人员估计该数据库公开可用的时间超过一年。

https://cybernews.com/security/powder-room-data-leak/

8、美国医疗服务公司发生数据泄露，影响超过 400 万人

3 月 22 日，美国医疗服务公司 Independent Living Systems (ILS) 披露了一起数据泄露事件，该事件暴露了超过 400 万人的个人和医疗信息。

安全漏洞是在 2022 年 7 月 5 日发现的，当时公司的某些系统变得无法访问。这种情况表明系统感染了勒索软件。该公司在外部网络安全专家的支持下对该事件展开了调查。调查显示，在 6 月 30 日至 7 月 5 日期间，威胁行为者可以访问某些系统。

数据泄露通知指出，受影响的信息类型因人而异，可能包括姓名、地址、出生日期、驾照、州身份证、社会安全号码、财务账户信息、医疗记录号码、医疗保险或医疗补助身份证明、CIN#、精神或身体治疗/状况信息、送餐信息、诊断代码或诊断信息、入院/出院日期、处方信息、账单/索赔信息、患者姓名和健康保险信息。

https://securityaffairs.com/143832/data-breach/independent-living-systems-data-breach.html

9、爱尔兰食品巨头都乐承认员工数据泄露

3 月 23 日，据外媒报道，总部位于爱尔兰的新鲜农产品跨国公司都乐透露，员工数据在二月份袭击该公司的勒索软件泄露中受到损害。

都乐在 30 个国家拥有近 38,000 名员工，去年公布的收入为 92 亿美元，这使其成为网络勒索者的一个有吸引力的目标。都乐在向美国证券交易委员会 (SEC) 提交的一份文件中表示，其在 2023 年 2 月遭受了勒索软件的攻击，并涉及未经授权访问员工信息。但该公司没有透露有多少员工受到此次安全事件的影响。

https://www.infosecurity-magazine.com/news/irish-food-dole-employee-data/

10、Mispadu 银行木马瞄准拉丁美洲：90000 多份凭证被盗

3 月 20 日，一个名为 Mispadu 的银行木马与多个针对玻利维亚、智利、墨西哥、秘鲁和葡萄牙等国家的垃圾邮件活动有关，其目的是窃取凭证并提供其他有效载荷。

https://thehackernews.com/2023/03/mispadu-banking-trojan-targets-latin.html

11、多伦多市确认数据被盗，Clop 声称对此负责

3 月 23 日消息，多伦多市是 Clop 勒索软件团伙在持续的 GoAnywhere 黑客活动中遭遇的最新受害者之一。通过利用 GoAnywhere 安全文件传输工具中的远程代码执行漏洞，Clop 声称迄今为止已成功入侵 130 多个组织。

“多伦多市已确认攻击者确实通过第三方供应商未经授权访问了城市数据。访问仅限于无法通过第三方安全文件传输系统处理的文件。市政府正在积极调查已泄露文件的详细信息。”多伦多市发言人表示道。

https://www.bleepingcomputer.com/news/security/city-of-toronto-confirms-data-theft-clop-claims-responsibility/amp/

《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