全球数据安全观察

总第 118 期 2022 年第 46 期

(2022.12.12-2022.12.18)

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、《扩大内需战略规划纲要（2022－2035 年）》印发

12 月 14 日，中共中央、国务院印发《扩大内需战略规划纲要（2022－2035 年）》。其中，在加快推动数字产业化和产业数字化部分提出了要建立完善跨部门跨区域的数据资源流通应用机制，强化数据安全保障能力，优化数据要素流通环境。

http://www.gov.cn/zhengce/2022-12/14/content_5732067.htm

2、《“十四五”扩大内需战略实施方案》发布

12 月 15 日，为深入贯彻落实《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》和《扩大内需战略规划纲要（2022—2035 年）》，《“十四五”扩大内需战略实施方案》制定并公布。在完善知识、技术、数据要素配置机制部分，明确提出要建立数据资源产权、交易流通、跨境传输、安全防护等基础制度和标准规范。

http://www.gov.cn/xinwen/2022-12/15/content_5732127.htm

3、《工业和信息化领域数据安全管理办法（试行）》印发

12 月 8 日，工业和信息化部印发《工业和信息化领域数

据安全管理办法（试行）》，从数据分类分级管理、数据全生命周期安全管理、数据安全监测预警与应急管理、数据安全检测、认证、评估管理等方面对工业和信息化领域的数据安全管理提出要求。

http://www.gov.cn/zhengce/zhengceku/2022-12/14/content_5731918.htm

4、《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》发布

12 月 16 日，全国信息安全标准化技术委员会秘书处发布了《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》，该规范从基本原则、个人信息处理者和境外接收方在个人信息跨境处理活动的个人信息保护、个人信息主体权益保障等方面提出了个人信息跨境处理活动安全认证要求。

http://xn--6oqtsz1bba48b68do6cv9hcth0ued0qr5fmurkyc.org/

5、通信行程卡用户数据将随“通信行程卡”服务下线同步删除

根据国务院联防联控机制综合组有关要求，12 月 13 日 0 时起，将正式下线“通信行程卡”服务。“通信行程卡”短信、

网页、微信小程序、支付宝小程序、 APP 等查询渠道将同步下线。中国信通院、三大运营商同步删除用户数据，依法保障个人信息安全。

https://m.gmw.cn/2022-12/13/content_1303223417.htm

6、杭州数据安全联盟首批加入杭州国际数字交易联盟

12 月 12 日下午，首届全球数字贸易博览会国际数字服务与数字产品交易论坛成功举办。论坛上，由杭州市数据资源管理局指导和牵头的“杭州国际数字交易联盟”正式成立，杭州数据安全联盟成为首批联盟发起单位。

https://mp.weixin.qq.com/s/VFjCnRs-ICfiS1XcGc7zkw

7、《关于欧盟-美国数据隐私框架的充分性决定草案》发布

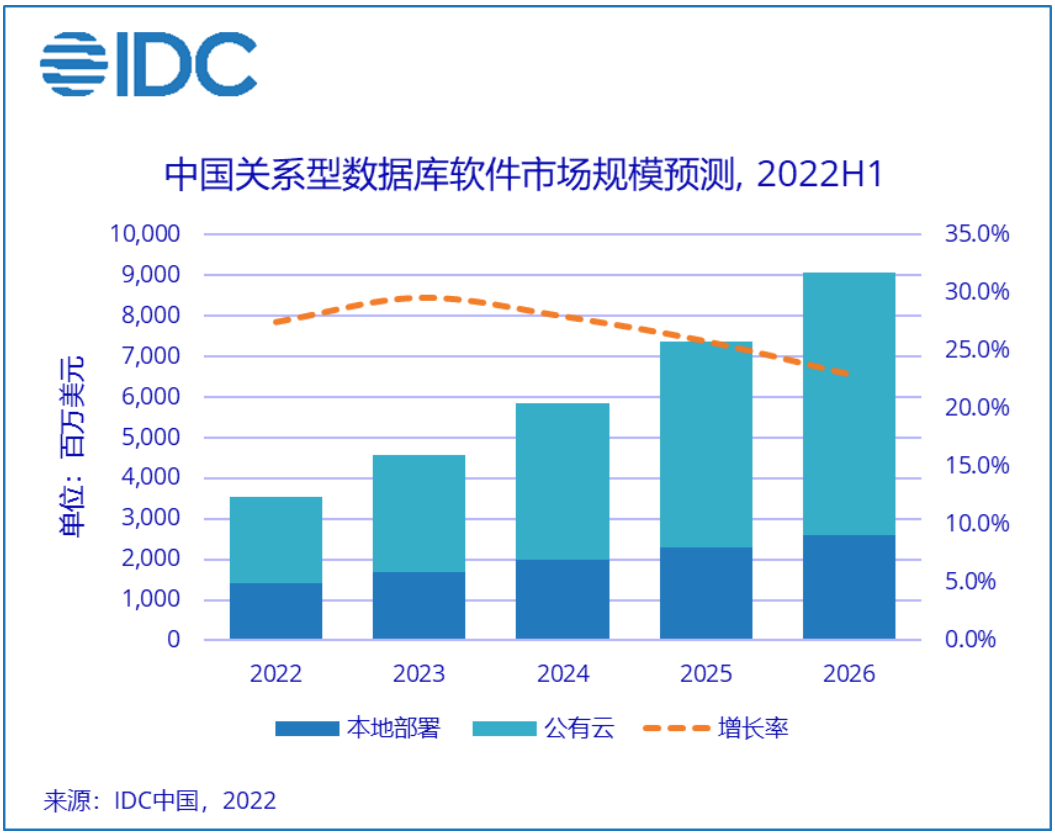
12 月 13 日，欧盟委员会启动了“欧盟-美国数据隐私框架充分性决定”（Adequacy decision for the EU-US Data Privacy Framework）的进程，并发布充分性决定草案。该框架将促进跨大西洋数据的安全流动，并试图解决欧盟法院在 2020 年 7 月 Schrems II 裁决中提出的担忧。

https://mp.weixin.qq.com/s/Ww2GnsyZEQx3E7boBpNzZw

技术、产品与市场

1、上半年，中国关系型数据库软件市场本地部署模式增速放缓

2022 上半年，受疫情的持续影响，企业和政府 IT 投资紧缩，大量 IT 建设项目延期或暂停，也造成了对数据库产品的采购量下降。相对公有云产品，本地部署模式的数据库产品受到的影响更大。IDC《2022 年上半年中国关系型数据库软件市场跟踪报告》显示，2022 上半年中国关系型数据库软件市场规模为 15.5 亿美元，同比增长 30.4%。其中，公有云关系型数据库规模 9.5 亿美元，同比增长 42.0%；本地部署关系型数据库规模 6.0 亿美元，同比增长 15.6%，与 2021 年同期相比增速下降 8.1%。IDC 预测， 到 2026 年，中国关系型数据库软件市场规模将达到 90.7 亿美元，2021-2026 的 5 年市场年复合增长率（CAGR）为 26.8%。



https://mp.weixin.qq.com/s/gwxA83XblO7WBb0Ha6vpyA

2、IDC 发布《中国数据安全服务市场洞察》：服务引领全流程数据安全体系建设

根据 IDC 统计，2021 年，全球创造了 82.5ZB 数据，未来五年，全球数据规模将以 21.2%的年复合增长率快速发展，到 2026 年，全球数据量将高达 216ZB。

本次研究 IDC 对众多安全厂商和最终用户进行了深入访谈，发现最终用户在其数据安全建设前或建设过程中普遍面临数据安全建设无从入手、摸清家底难、分类分级落地难、对于数据安全风险和建设成果的无感知以及缺乏专业的数

据安全建设治理人才等问题。针对以上痛点，IDC 给出以下几点建议供技术买家参考:

（1）数据安全体系建设是“一把手”工程。

（2）数据安全需体系化、阶段化、模块化建设。

（3）清晰、明确的组织架构和管理制度是企业数据安全体系建设的“地基”。

（4）分类分级、数据治理是组织建好、管好数据安全的前提。

（5）数据安全建设需服务先行。

（6）数据安全教育和培训是一件需要长期坚持的事。

https://www.secrss.com/articles/49934

3、继公布开源计划之后，谷歌又推出最大的开源漏洞数据库

当地时间 12 月 13 日，谷歌宣布开源 OSV-Scanner，该开源漏洞扫描仪可访问各种项目的漏洞信息，加强软件供应链安全。

谷歌软件工程师 Rex Pan 向媒体介绍，该工具基 Go 语言编写，由开源漏洞（OSV）数据库提供支持，可以生成可靠和高质量的漏洞信息，填补了开发人员的软件包清单与漏洞数据库信息之间的空白。

扫描仪的原理是利用从 OSV.dev 数据库中提取的数据，

来识别一个项目的所有横向依赖关系同时突出相关的漏洞。

OSV.dev 数据库拥有 3.8 万个共建者，支持 16 个生态系统，包括所有主要语言、Linux 发行版（Debian 和 Alpine）、安卓、Linux 内核和 OSS-Fuzz。安全告警数量比一年前的 1.5 个多，其中 Linux（27.4%）、Debian（23.2%）、PyPI（9.5%）、Alpine（7.9%）和 npm（7.1%）占据告警量前五。

下一步，谷歌计划建立一个“高质量数据库”来支持 C/C++漏洞，包括向 CVEs 添加 “精确的提交级元数据”。

https://www.freebuf.com/news/352442.html

4、研究：2022 年 10 大医疗保健数据泄露事件中的大多数都与供应商有关

据 SC Media 的研究调查结果显示，今年报告的 10 大医疗保健数据泄露事件中有 90% 是由第三方供应商造成的，这与 2021 年非常相似，其中许多网络攻击的后果对多个相互连接的提供商造成了影响。

这些事件应作为重新审视第三方供应商关系的警告，确保实体至少每年对供应商进行一次审查，并在可能的情况下考虑整合供应商。

https://www.scmagazine.com/feature/breach/most-of-the-10-largest-healthcare-data-breaches-in-2022-are-tied-to-

vendors?&web_view=true

5、杭州国际数字交易中心正式揭牌，累计实现交易金额 10.91 亿元

12 月 12 日，首届全球数字贸易博览会之江数字贸易论坛在杭州国际博览中心举行。在论坛上，杭州国际数字交易中心揭牌，意味着杭州国际数字交易中心正式亮相。依托杭州数字经济和信息产业领域的创新力优势，杭数交通过深耕数据要素业务与数字资产业务，探索建立数字交易制度体系，推动数字经济深化发展，以实现生产加工数字化、交易方式数字化，构建具有国际影响力的开创性数字交易平台。遵循数字经济发展，合法合规先行的要求，杭数交打造“3+1+N”数字交易平台。建设 3 个平台，形成一套全面易行、高效可信的交易体系规范，致力于解决数据生产及交易过程中的一系列合规性问题。N 为打造 N 个高社会价值、具有试点效应的应用场景。

截至目前，杭数交已与 215 家企业建立合作关系，上架产品 428 件，实现 568 笔交易业务，累计实现交易金额 10.91 亿元。

https://mp.weixin.qq.com/s/oulG-ytDq4M1_qo_RVPAvw

业界观点

1、贯彻总体国家安全观，构建数字政府全方位安全保障体系

在数字政府的建设过程中，必须时刻坚持底线思维，将数据安全防护的关口前移，构建全流程、全周期、全场景的数据安全管理制度。**一是构建全流程的数据安全管理制度。**在识别和划分各类数据安全事件的基础上，建立事前、事中和事后的全流程数据安全管理制度，形成动态优化的闭环管理机制。**二是构建全周期的数据安全管理制度。**政务数据的归集、使用以及管理需要建立在全周期的数据安全管理制度基础上，确保在各个阶段“谁拥有，谁负责”“谁使用，谁负责”以及“谁流转，谁负责”。**三是构建全场景的数据安全管理制度。**除通过法律和技术解决数据安全问题，还要加强从数据使用场景入手规范数据的使用与管理，规避和控制因人为失误引发的安全风险。

全方位提升数据安全保障能力，要坚持安全可控的基本原则，加强数据安全产业新产品、新技术、新范式与新机制的应用，以自主创新为驱动，攻克数字政府领域的关键核心技术，全面构建制度、管理和技术衔接相配套的安全防护体系，守住数字政府的数据安全底线。**一是坚持安全可控。**坚定不移贯彻总体国家安全观，坚持促进发展和依法管理相统

一、安全可控和开放创新并重，建立常态化、高频率和全方位的数据安全检查工作机制，根据网络安全形势的变化，拓展网络安全态势感知监测范围，加强大规模网络安全事件、网络泄密事件预警和发现能力。**二是加强技术应用。**进一步加强各类数据安全技术的应用，建立健全动态监控、主动防御、协同响应的数字政府安全技术保障体系。充分借鉴其他地区的应用实践，积极开展前沿技术的试点应用。**三是加强自主创新。**以自主创新为驱动，加快数字政府建设领域关键核心技术攻关，推广应用安全可靠的自主科技成果。同时，推动公职人员与科研团队建立沟通反馈机制，促进对新技术新应用的技术优化与自主品牌的服务提升，切实提高自主可控水平。

建立健全数据安全人才培养体系，要以加强领导干部安全教育为抓手，以提高全民数据安全意识和素养为目标，以培养复合型安全人才为核心，筑牢人民防线。**一是加强数据安全教育培训。**一方面，要定期面向各级领导干部开展数据安全教育培训，持续提升干部队伍的数据安全意识；另一方面，要加大对安全教育的财政投入与政策支持力度，引导高校和科研院所设置网络空间安全相关专业与课程，推动更多的企业开发和完善数据安全教育培训体系。**二是加强复合型安全人才的培养力度。**要建立政府主导、学校企业为主体、

行业协会为中介的人才培养模式，鼓励政府与企业的有关人员深度参与高校课程建设，利用行业协会资源优势，为人才创造更多的实战演练与实习交流机会。将校企的科技创新过程与人才培养项目相结合，全面提升数据安全后备人才的攻防实战能力，建设一支懂业务、精技术的复合型人才队伍。**三是加强数据安全人才选拔使用。**建立健全数据安全人才引进、选拔与激励机制，确保人才引得进、用得好、留得住。出台高层次安全人才引进政策，优化落户、购房、专项资金等条件。通过招考遴选、攻防竞赛和跟踪考察等方式选拔优秀数据安全人才，依托人才需求建立和完善正向激励机制，拓宽和畅通人才晋升渠道，吸引和鼓励更多数据安全人才参与数字政府建设。

http://www.echinagov.com/viewpoint/333726.htm

2、余晓晖：构筑顶层设计，开创工业和信息化领域数据安全管理新格局

近日，工业和信息化部出台了《工业和信息化领域数据安全管理办法（试行）》，中国信通院余晓晖对此进行了解读。

一、夯实数据安全根基，建立工信领域数据安全管理基本遵循

加速完善工信领域数据安全管理政策，夯实数据安全工

作基石，是认真践行总体国家安全观，统筹发展和安全，护航工信领域数字化发展的必然要求，也是落实党和国家决策部署、提升国家总体数据安全保障水平的必担之责。

二、筑牢数字安全屏障，明确工信领域数据安全保护的规则指引

《管理办法》坚持安全与发展并重、鼓励与规范并举原则，推动建立健全安全可控、弹性包容的工信领域数据安全规则体系，一方面，明确数据安全管理关键制度要求，划定工信领域数据流通利用的安全基线，同时，构建多元主体协同共治格局，着力提升工信领域数字信任，为我国数字化转型保驾护航。具体来说,《管理办法》核心内容包括以下几个方面:

（一） 明确管理体制,建立三级联动的数据安全工作机制;

（二） 细化分类分级,建立涵盖事前事中事后的监管制度机制;

（三） 落实主体责任,加强重要数据和核心数据重点保护;

（四） 引入多利益相关方,构建数据安全协同治理生态。

三、凝聚多方合力，全面提升工信领域数据安全保障水平

《管理办法》正式实施后，将开创工信领域数据安全保护工作新局面。为进一步推动其落地，有效提升工信领域数据安全治理能力，重点提出以下几方面思考：

（一）加强政策宣贯培训，全面提升数据安全保护意识和水平；

（二）做好重要数据识别备案，有效夯实数据安全工作基础；

（三）抓好风险防范化解，切实增强数据安全保障能力；

（四）加强正向激励引导，多措并举提升数据安全保护水平。

https://freewechat.com/a/MjM5MzU0NjMwNQ==/2650826345/1

3、韦韬：数据密态时代多久到来

近日，蚂蚁集团副总裁兼首席技术安全官韦韬博士接受采访时表示，“只要数据流通是处于明文状态，那么往往因为明文分发易失控导致数据泄露，加剧数据滥用，甚至引发数据要素的价值崩塌。迈进‘数据密态’时代，对数据要素的跨域流转实现全程安全可控，已经成为建设数字要素市场、发展数据要素经济的必然一步。”

他指出，目前可信隐私计算是实现数据密态呼声最高的

技术路径之一，可以实现在不丧失数据持有权的前提下，有效实现数据使用权的跨域管控。隐私计算产品安全性度量的本质在于需要付出多大的成本、克服多大的不确定性来攻破给定的安全防护保障，造成信息泄露的后果或风险。在这个认知的基础上，正在尝试将隐私计算产品安全从实战角度划分为基线防护级、审计追溯级、广度防护级、深度检验级、安全证明级五个等级。

韦韬表示，数据密态时代会经过计算密态化、大数据密态化、数据要素密态化等三个阶段。

“计算密态化”阶段，指的是各个机构出于业务发展的最急迫需求，在最核心的几个场景开始尝试密态计算，通过联邦学习、MPC 等隐私保护技术，开展最基础的计算、分析、建模等工作，相对固定且复杂度有限。

在“大数据密态化”阶段，数据密态处理将越来越多地呈现出大数据处理的特点，包括留存大量的中间结果以供后续的环节使用。

在“数据要素密态化”阶段，在数据持有权和使用权分离的基础上，实现多方、异构互联。同一份数据持有权仅由最初的机构拥有，其他机构仅能获得使用权，避免数据被到处复制、留存。除此之外，还需要解决数据的定价、平台的公信力等问题。

韦韬还指出，目前密态时代仍处于第一阶段，未来有着极其广阔的发展前景。同时，密态时代发展所面临的技术挑战既涉及的维度多，又有非常大的难度。因此，密态时代需要一个兼顾高安全、高性能、高稳定性、高适用性、低成本等多方面能力的技术方案，为数据价值的充分挖掘提供坚实底座。在技术要求方面，数据密态时代到来的标志性事件有五个衡量标准：一是性能强大，要达到每小时处理亿级样本数据建模；二是可靠稳定，在关键应用领域要够达到 99.99%的标准；三是成本足够低，要让企业普遍负担得起；四是适用性广，要做到覆盖全场及和支持不同处理逻辑；五是安全性足够高，能够有效抵抗实战威胁，为行业发展提供有效保障。

https://www.36dianping.com/dianping/5494020121

4、人工智能应用面临 7 大数据安全威胁

日前，安全研究人员梳理总结了目前人工智能技术在实践应用中经常要面对的 7 个数据安全威胁。

威胁 1：模型中毒

模型中毒（Model poisoning）是一种对抗性攻击形式，旨在操纵机器学习模型的结果。威胁行为者可以尝试向模型中注入恶意数据，进而导致模型对数据进行错误分类并做出

错误的决策。

为了防止恶意行为者篡改模型输入，企业组织应该实施严格的访问管理策略来限制对训练数据的访问。

威胁 2：隐私泄露

隐私保护是一个敏感的问题，需要额外的关注和重视，尤其是 AI 模型中包含有未成年人的数据时，问题就更复杂了。

企业组织必须定期进行安全审计，并在人工智能开发的所有阶段实施强有力的数据保护实践。隐私风险可能发生在数据生命周期的任何阶段，因此为所有利益相关者制定统一的隐私安全策略非常重要。

威胁 3：数据篡改

数据操纵、暴露和篡改所带来的风险，在 AI 规模化应用背景下正在被不断放大，因为这些系统需要基于大量数据进行分析决策，而这些数据很容易被恶意行为者操纵或篡改。此外，算法偏见是人工智能规模化应用中所面临的另一个主要问题。人工智能算法和机器学习程序应该是客观和公正的，但事实却并非如此。

人工智能算法的数据篡改威胁是一个巨大的问题，这没有简单的解决方案，但它需要引起重视。

威胁 4：内部威胁

就数据安全而言，来自内部威胁无疑是最危险的一种，也是代价最高昂的一种类型。根据最新的《内部威胁成本：全球报告》显示，在过去两年中，内部威胁事件的数量上升了 44%，每起事件的平均损失成本为 1538 万美元。

内部威胁之所以如此危险，是因为他们的动机不一定是金钱，还可能是出于报复、好奇心或人为错误等其他因素。正因如此，它们比外部的攻击者更难预测和阻止。

威胁 5：针对性蓄意攻击

“蓄意攻击”是指有目的地通过侵入人工智能系统来破坏一个组织的业务运作，目的是获取领先于对手的竞争优势。在蓄意攻击场景中，对 AI 和 ML 的数据安全威胁可能尤其具有破坏性。因为这些系统中使用的数据通常是专有的，具有很高的价值。当人工智能系统遭到针对性的蓄意攻击时，其后果不仅仅是数据被窃取，而是公司的竞争能力被破坏。

威胁 6：大规模采用

随着 AI 应用越来越受欢迎，并在世界范围内被采用，黑客将会找到新的方法来干扰这些程序的输入和输出。

保护企业免受大规模应用威胁的最佳方法是结合良好的编码实践、测试流程，并在发现新漏洞时及时更新。当然，不要放弃传统形式的网络安全预防措施，例如使用托管数据中心来保护服务器免受恶意攻击和外部威胁。

威胁 7：AI 驱动的攻击

研究人员发现，恶意攻击者正在将人工智能武器化，帮助他们设计和实施攻击。在这种情况下，“设计攻击”指的是选择一个目标，确定他们试图窃取或破坏什么数据，然后决定一种传输方法。非法攻击者可以使用机器学习算法寻找绕过安全控制的方法来进行攻击，或者使用深度学习算法，根据真实世界的样本创建新的恶意软件。安全专家必须不断防御愈发智能的机器人，因为一旦他们阻止了一种攻击，另一种新的攻击就会出现。简而言之，人工智能使攻击者在当前安全保障措施中寻找漏洞变得更容易。

https://www.secrss.com/articles/49940

5、银行数据安全治理模型

近日，在 2022（第二届）金融合规与风控管理高峰论坛上，国金融认证中心(CFCA) 华东分公司副总经理马关尔指出，银行数据安全治理模型应当从各个层级及过程的不同关注点出发，按照治理层、管理层、控制层的关注内容进行设计。

从治理层面来讲，应当关注和输入法规和监管、相关行业标准以及业内实践范式，确定组织构架、策略规范、技术保障、人员建设和风险控制五个范畴的政策、原则。

从管理层面来讲，按照一般管理的三个层次即制度建设、绩效建设、文化建设，将治理层的安全政策、策略等落实到具体的管理过程之中。

从控制层面来讲，主要关注具体可落地的策略或信息系统层面的问题，落实的抓手就是数据的生命周期控制。

https://www.sohu.com/a/617587293_115643

数据安全事件

1、勒索团伙 LockBit 称已从加州财政部窃取 75.3 GB 的数据

据 12 月 12 日报道，LockBit 声称已入侵加利福尼亚州的财政部，并窃取了数据库、机密数据、财务文件和 IT 相关的文件。攻击者还发布了目录和存储文件数量的截图，显示超过 114000 个文件夹中有超过 246000 个文件，总计 75.3GB 的数据。目前，LockBit 要求的赎金金额尚不清楚，但是其网站的倒计时显示要在 12 月 24 日之前付。加州州长紧急服务办公室表示，加州网络安全集成中心（Cal-CSIC）正在积极应对此事件，但没有提供太多细节信息。

https://www.cyberscoop.com/lockbit-ransomware-california-department-of-finance/

2、哥伦比亚能源供应商 EPM 遭受 BlackCat 勒索软件攻击

12 月 17 日报道，哥伦比亚能源公司 Empresas P ú blicas de Medell í n (EPM) 当地时间 12 月 12 日（周一）遭受了 BlackCat/ALPHV 勒索软件攻击，扰乱了公司的运营并中断了在线服务。EPM 是哥伦比亚最大的公共能源、水和天然气供应商之一，为 123 个城市提供服务。

EPM 向当地媒体透露 ，他们正在应对一起网络安全事件，并为客户提供了支付服务费用的替代方法。检察官办公室后来证实勒索软件是 EPM 网络攻击的幕后黑手，导致设备被加密和数据被盗。

据调查，被破坏的信息不包含客户数据，而是包含公司的运营和内部动态。但专门从事此类犯罪的 Mucho Hacker 门户网站发布的屏幕截图将证明存在有关员工和财务信息的私人数据，例如有关付款、预算、报告、报告和银行文件的数据。检察官办公室估计，从 EPM 窃取信息的规模将达 15T。

https://www.secrss.com/articles/50129

3、Social Blade 在黑客发布被盗用户数据后确认违规

12 月 15 日，据外媒报道，社交媒体分析平台 Social Blade 证实，在其数据库遭到破坏并在黑客论坛上出售后，他们遭受了数据泄露。

Social Blade 是一个分析平台，可为 YouTube、Twitter、Twitch、Daily Motion、Mixer 和 Instagram 帐户提供统计图表，让客户可以查看预估收入和项目。该公司提供了一个 API，允许客户将 Social Blade 数据直接集成到他们自己的平台中。

在 BleepingComputer 联系 Social Blade 关于出售他们数据的事件后，该公司确认他们遭受了数据泄露，并开始向客户发送数据泄露通知。此数据泄露通知指出，黑客成功访问了公司的数据库并窃取了以下信息：电子邮件地址、密码哈希、客户端 ID、商业 API 用户的令牌、连接帐户的授权令牌、各种非个人和内部数据。

https://www.bleepingcomputer.com/news/security/social-blade-confirms-breach-after-hacker-posts-stolen-user-data/?&web_view=true

4、国际乒联泄露数百名运动员护照和疫苗接种证书

2022 年 12 月 14 日，由于国际乒乓球联合会（ITTF）的服务器出现安全问题，数百名乒乓球运动员的护照细节和疫苗接种证明等信息被泄露，其中包括中国运动员马龙和樊振东的信息。

https://cybernews.com/news/table-tennis-athletes-passport-vaccination-details-leaked/

5、加州信用卡处理公司因配置错误 900 万条交易记录泄露

12 月 13 日消息，研究团队发现了一个未受保护的数据库，其中包含 9098506 条信用卡交易记录。更糟糕的是，个

人和财务信息也被暴露在配置错误的服务器上，没有任何密码或安全身份验证。该数据库被确定属于 Cornerstone Payment Systems，这是一家位于加利福尼亚的信用卡处理公司。该事件泄露了信用卡号、账户或交易信息、姓名、安全或访问令牌以及交易信息等，可被用来进行钓鱼攻击。获悉问题后，该公司立即采取行动保护服务器。

https://www.hackread.com/exposed-credit-card-transaction-records/

6、黑客在暗网上出售 FBI InfraGard 数万用户的数据库

据 12 月 13 日报道，InfraGard 的 80000 多名成员的联系信息数据库在暗网 Breached 上被公开出售。同时，黑客还通过 InfraGard 门户网站直接与会员进行在线交流，并使用一个由 FBI 自己审核的金融业 CEO 的假身份的新账户。InfraGard 是 FBI 运行的一个项目，旨在与私营部门建立网络和物理威胁信息共享合作关系。FBI 表示，它已经知道潜在的虚假账户，并正在积极调查此事，目前无法提供任何额外信息。

https://krebsonsecurity.com/2022/12/fbis-vetted-info-sharing-network-infragard-hacked/

7、电信公司 TPG Telecom 上万个客户邮箱遭到未授权访问

路透社 12 月 14 日报道称，澳大利亚电信公司 TPG Telecom 遭到网络攻击，多达 15000 个企业客户的电子邮件被未授权访问。TPG 表示，黑客攻击托管交易所服务的主要目的是为了搜索客户的加密货币和金融信息。该公司表示已采取措施阻止未经授权的访问，并正在联系所有受此事件影响的客户。其股价受此消息影响下跌，收盘下跌 2.8%。自 10 月以来，至少有 8 家澳大利亚公司遭到了黑客攻击。

https://www.reuters.com/world/asia-pacific/tpg-telecom-finds-evidence-unauthorised-access-up-15000-email-accounts-2022-12-13/

8、Uber 因第三方供应商遭到攻击源代码和员工信息等泄露

据媒体 12 月 12 日报道，黑客 UberLeaks 在论坛上发布了从 Uber 和 Uber Eats 窃取的数据。泄露的数据包括源代码、IT 资产管理报告、数据销毁报告、Windows 域登录名以及超过 77000 个 Uber 员工的信息等。研究人员最初认为这些数据是在 9 月份的攻击事件中被盗的，但 Uber 表示这与第三方供应商的安全漏洞有关。Uber 表示，用于资产管理和跟踪服务的 Teqtivity 遭到攻击，攻击者获得了其为客户存储数据的 Teqtivity AWS 备份服务器的访问权限。

https://www.bleepingcomputer.com/news/security/uber-suffers-new-data-breach-after-attack-on-vendor-info-leaked-online/

9、印度外交部泄露其海外居民的护照详细信息

据 Cybernews 12 月 13 日的报道，其研究团队收到报告，说是印度外交部专门负责联络海外印度侨民的 Global Pravasi Rishta Portal 平台泄露了用户敏感的护照详细信息。Cybernews 在调查后证明确有其事。

Global Pravasi Rishta Portal 门户网站旨在作为外交部、印度使团和印度侨民之间沟通的工具，其目标是连接 3000 万印度外籍人士。该平台所有者是印度外交部，该国负责实施外交政策的政府机构。

据悉，Global Pravasi Rishta Portal 以明文形式公开了注册用户的用户名、姓氏、电话、电子邮件地址，职业状态、护照号码和居住国。该数据泄漏可能是由于安全措施不佳，例如缺乏身份验证方法。

https://www.wangan.com/news/11v6c4ed258a78c9

10、第三方供应商数据泄漏，Gemini 客户恐遭钓鱼攻击

12 月 16 日报道，Bleeping Computer 网站披露，Gemini 加密货币交易所近日宣布，由于第三方供应商遭网络攻击，

导致大量客户的电子邮件地址和电话号码泄露，部分 Gemini 客户可能已经成为了潜在网络犯罪分子的攻击目标。

第三方供应商数据泄露事件不久后，Gemini 产品安全团队在一份安全通知中表示，客户数据信息泄露原因是第三方供应商遭遇了一次 "网络安全事件"，导致部分 Gemini 客户电子邮件地址和不完整的电话号码泄露。基于上述情况，部分 Gemini 客户收到了钓鱼电子邮件。

在某个黑客论坛上出现了多篇出售 Gemini 数据库的帖子，数据库中包含了 570 万用户的电话号码和电子邮件地址。值得一提的是，之前某黑客论坛上已经有攻击者尝试出售数据库，并标价 30 个比特币（按当前汇率计算约 52 万美元）。

https://www.bleepingcomputer.com/news/security/hackers-leak-personal-info-allegedly-stolen-from-57m-gemini-users/

11、加州医院泄露事件暴露了患者的社会安全号码和医疗信息

12 月 13 日，据外媒报道称，加利福尼亚州河滨县的一家医院向其患者报告了数据泄露事件，包括社会安全号码等敏感信息以及秋季事件后的医疗护理细节。

根据该通知，从 10 月 29 日开始，“未经授权的一方”

访问了位于班宁小镇的非营利性机构 San Gorgonio 纪念医院的计算机网络，当时检测到漏洞并隔离并关闭了“选定”网络系统。

“此时，我们已经确定了包含患者姓名、地址、出生日期、病历号、就诊 ID 号和/或临床信息（例如服务日期、提供者名称和/或部门名称）的文件遭受泄露，”医院在通知中写道。“在某些情况下，患者的社会安全号码、驾照号码、财务账户信息和/或健康保险信息也可能反映在所涉及的文件中。”

https://therecord.media/california-hospital-breach-exposed-patients-social-security-numbers-medical-info/?web_view=true

12、HHS 报告第三方供应商事件泄露了 254K 的健康数据

12 月 15 日报道，美国卫生与公共服务部医疗保险和医疗补助服务中心（HHS）目前通知其 6400 万医疗保险受益人中的 254,000 人，他们的数据在其第三方供应商之一遭到勒索软件攻击后遭到泄露。

该事件凸显了医疗保健行业在供应商管理方面面临的持续挑战，因为今年报告的大多数最大事件都与业务合作伙伴有关。总体而言，该行业依赖大量第三方供应商和业务伙伴来维持日常运营。但每增加一份合同都会进一步扩大威胁

范围，近年来外包服务的增加和大量关键基础设施攻击加剧了威胁范围。

此次事件泄露的数据可能包括姓名、出生日期、社会安全号码、联系方式、医疗保险受益人标识符、银行信息、医疗保险权利信息、登记和保费。

https://www.scmagazine.com/analysis/third-party-risk/hhs-reports-third-party-vendor-incident-compromised-health-data-of-254k?&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： 唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nercbds@163.com

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