全球数据安全观察

总第 129 期 2023 年第 10 期

(2023.03.13-2023.03.19)

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、《新时代的中国网络法治建设》白皮书发布

3 月 16 日，国务院新闻办公室发布《新时代的中国网络法治建设》白皮书，旨在全面介绍中国网络法治建设情况，分享中国网络法治建设的经验做法，为全球互联网治理贡献了中国智慧和中国方案。

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

2、《关于推动北京互联网 3.0 产业创新发展的工作方案（2023-2025 年）》印发

3 月 17 日，北京市科学技术委员会、中关村科技园区管理委员会印发《关于推动北京互联网 3.0 产业创新发展的工作方案（2023-2025 年）》，从互联网 3.0 基础设施层与交互终端层、互联网 3.0 平台工具层、典型应用场景、互联网 3.0 创新生态构建、互联网 3.0 风险监管等方面提出重点任务。其中，针对互联网 3.0 监管，提出聚焦互联网 3.0 内容监管、数据安全、隐私保护、身份可信、资产确权等，加强监管机制和监管模式探索，利用区块链、隐私计算、网络安全、量子加密等新型监管技术，实现对互联网 3.0 虚拟世界的可监管和可审计，保障互联网 3.0 数据的安全与隐私，提升对虚拟

世界监管的智能化水平。

http://kw.beijing.gov.cn/art/2023/3/17/art_736_639986.html

3、甘肃省出台《关于促进数据要素市场发展的实施意见》

近日，甘肃省委、省政府印发了《关于促进数据要素市场发展的实施意见》，明确了数据要素市场培育建设目标、重点任务和保障措施，为数据要素安全流通、公平交易、高效配置提供了政策保障，将有效促进公共数据开放应用、社会数据高效流通，释放公共数据价值，激发社会数据活力，引导数据资源汇聚融合与创新应用，为我省培植壮大经济发展新动能、提高数字经济发展质量提供重要支撑。

https://mp.weixin.qq.com/s/c1DA_S7RlmF4_XWLMlp0MQ

4、《数字宁夏“1244+N”行动计划实施方案》印发

3 月 14 日， 宁夏回族自治区人民政府办公厅印发《数字宁夏“1244+N”行动计划实施方案》，围绕数字宁夏建设，推动实施“1244+N”行动计划，健全完善组织、规划、政策保障体系，加快全国一体化算力网络国家枢纽宁夏节点和国家（中卫）新型互联网交换中心建设，大力实施数字产业化、产业数字化、数字化政务、数字化社会“四化”工程，加快推动经济社会高质量发展。

https://www.nx.gov.cn/zwgk/qzfwj/202303/t20230313_3991964.html

5、信安标委正式发布《个人信息跨境传输认证要求》征求意见稿

3 月 16 日，全国信息安全标准化技术委员会秘书处发布《信息安全技术 个人信息跨境传输认证要求》征求意见稿，规定了个人信息处理者跨境提供个人信息的基本原则、基本要求和个人信息主体权益保障要求。

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

技术、产品与市场

1、2022 年超过 7 亿个账户信息被泄露，2200 万台设备被感染

根据 SpyCloud 公布的《2023 年度身份暴露报告》，安全人员在 2022 年从各大事件中累计发现了 7.215 亿个账号信息被泄露，全球超过 2200 万台设备感染了恶意软件。

报告中指出，泄露的账号信息中，50% 来自于僵尸网络。这些工具通常用于部署高度准确的信息窃取恶意软件，信息窃取程序使网络犯罪分子能够大规模工作，窃取有效凭证、cookie、自动填充数据和其他有价值的信息，展开有针对性的攻击或在暗网上出售获利。

研究人员调查中发现了 86 亿个个人身份信息资产，其中包括 14 亿个全名、3.32 亿个国民身份证/完整的社会安全号码和 6700 万个信用卡号码。

报告中还发现了 220 亿个设备和会话 cookies，这些记录允许犯罪分子绕过 MFA 并劫持活动会话，从而使他们能够访问敏感信息。

尽管近年来越来越重视安全培训，但密码使用习惯仍然很糟糕。IT 之家从报告中获悉，在 2022 年泄露的用户密码中，有 72% 仍在重复使用之前泄露的密码。

https://spycloud.com/resource/2023-annual-identity-exposure-report/

2、浙商证券：数据安全市场产业调研报告

在我国数据安全防护和数据开发利用并重的数据安全监管格局下，数据安全市场正从传统以数据承载环境为中心的“系统视角”向以数据全生命周期流转为中心的“业务视角”转变，逐步演进为独立的赛道。在此背景下，我们认为数据安全赛道市场具有广阔成长空间，2025 年市场天花板接近千亿元，2019-2025 年复合增长率可达 67%。

数据安全监管框架：防护与开发并重，未来 2-3 年落地可期。2020 年 6 月发布的《数据安全法》（草案）预示着我国进入数据安全战略全面落地时期，受到政策实施、试点开展、以及产业指引三方面因素驱动，我们认为数据安全未来 2-3 年落地可期。

数据安全市场发展趋势：从“系统视角”到“业务视角”，追求更高回报率。未来数据安全市场有望沿着三个趋势发展：1）**更高的安全投资回报**，即从事后、外挂式的数据安全防护演变至涵盖事前事中事后、与业务紧耦合式的数据安全防护；2）**更合规的数据开发**，即借助隐私计算等技术手段，在保障数据“可用不可见”的前提下实现数据共享；3）**更轻量化的数**

据安全改造，即在补齐存量系统数据安全短板时尽量减少对前端业务的影响，降低改造成本和复杂度。

数据安全市场空间：考虑“数据二十条”，中短期 186 亿元，长期近千亿空间。若从中国数据总量在全球数据量的占比来看，考虑数据量增加和数据安全渗透率的提升，我们预计 **2025 年数据安全市场潜在空间有望达到 820 亿元，相较于 2019 年复合增长率为 67%**。若从“数据二十条”中数据要素基础制度带来的潜在增量市场来看，我们预计中短期（数据要素市场探索建设期，预计 2023-2025）市场增量需求约为 **186 亿元**，远期（数据要素市场成熟落地期，预计 2025-2030）市场增量需求接近**千亿元**。

安全厂商布局：各有侧重，自有产线布局和战略投资并行。通过对部分安全厂商在数据安全领域布局的梳理，我们发现：1）网安厂商在数据安全领域的布局节奏自 2020 年开始显著加快，且布局侧重点大致分为整体解决方案以及聚焦特定行业两类；2）头部安全厂商大多从自身优势领域切入数据安全赛道进行落地，随后进行扩展布局；3）除基于自身行业和技术优势发布自有产品及解决方案外，头部厂商还通过战略投资创业公司的方式进行布局。

数据安全投资框架。**需求侧**，建议短期跟踪政策变化，长期关注数据交易带来的商业模式变化；**供给侧**，建议关注

厂商布局产品结构和产品矩阵协同，产品布局前瞻或行业聚焦深入的公司有望获得更高胜率。

https://data.eastmoney.com/report/zw_industry.jshtml?infocode=AP202303131584212571

3、数世咨询：《数据访问安全域能力白皮书》全文发布

数世咨询认为，目前的数据安全正在由数据资产安全迈入数据访问和使用安全的时代——针对存储阶段的数据安全防护固然重要，其他阶段的数据安全也需要给予更多的重视；数据泄漏要面对的也不再仅仅是外部的黑客攻击，还包括内部员工、合作伙伴使用和交换数据时的数据失泄密行为。

鉴于此，数世咨询提出一个全新的细分领域——“数据访问安全域”，主要关注的是数据访问过程中如何实现对数据的安全管控这一需求。

通过梳理，数世咨询认为现有的数据访问安全技术方案，其基座来源于“网络安全”，侧重于网络攻防，即通过分析数据安全链路的风险点，在数据可能的流通路径上进行埋点检测，通过数据加解密、软件策略、威胁检测等手段进行保护，传统的 DLP、EDR、终端安全软件等都是基于这种思路实现。这样的实现方式，能够解决大部分数据访问的安全问题，但仍然会存在数据资产盘点不清，数据流通路径不明，数据访

问管理不完整等盲区。

基于此，数世咨询认为应当以数据访问场景为脉络，建立安全、隔离的数据空间，在该空间中完成数据的访问、传输、共享、删除、追溯等全程管理，以此保护数据资产安全、共享流通以及数据访问的安全。

https://mp.weixin.qq.com/s/RKAmj7uhwnoKmNfXAt0DIQ

4、首笔可信数据空间技术商业化案例正式落地

由长虹控股、深圳数据交易所、数鑫科技与中国信息通信研究院四方携手共创的国内首笔场内数据空间业务合作，以自主可控的可信数据空间（Trusted Data Matrix，简称 TDM）架构为基础，融合区块链、物联网和零信任等先进技术，通过有机结合国内现有消费电子行业企业数据流通特点、实际应用场景、数据保护及交易法规等，实现质量数据可信流通，消费电子产品、新能源锂电池等生产全过程质量数据可信共享，有效解决数据协同策略难统一，数据使用难监控，发生事件难溯源等诸多数据安全及管控具体问题，进而支撑产业链上下游全过程实时柔性双向质量追溯，进一步促进了质检前置，大幅提升客户满意度。

https://mp.weixin.qq.com/s/gkPh13qpzDdM98TPsSgSBA

5、中国移动牵头定义“1 个技术底座+X 个厂商算法”隐私计算平台

日前，中国移动牵头组织业内技术伙伴联合编写并发布《中国移动“1+X”隐私计算平台纳管集成规范》，主要基于1+X 架构的互联互通分级纳管模式展开说明。其中“1”为一个技术底座，“X”为多个厂商算子算法，是将异构算法互联互通、快速集成，通过集成其它数据参与方或需求方的算子算法实现平台的开放互通。

基于中国移动“1+X”架构的隐私计算平台，在异构隐私计算平台中，通过管理系统、算法协议及计算原语的松耦合设计，支持「黑盒」、「白盒」、「灰盒」多种互通模式，进而实现递进式互联互通的安全可视化，提高了安全层面的可解释性，让用户掌握更强的系统运营能力。从黑盒变成灰盒，灰盒变成白盒，多种互通模式的转变实现了多边信任增强，提升了各行业隐私计算互通效率。

https://mp.weixin.qq.com/s/p3DFOlSIFavGs0JTTv4CPg

业界观点

1、全国政协委员连玉明：组建国家数据局将带来三大变化

十八大以来，特别是2018年开始的地方机构改革，地方政府设立大数据管理局是机构与行政体制改革一项新实践。此次，国务院机构改革方案中提出组建国家数据局，是在国家层面上推进政府数据治理的组织化表现，也是完善国家宏观数据治理体系，提升数据治理能力的重要举措。

国家数据局的组建，预计将会带来三大主要变化：**一是有利于职能任务的集中化**。国家数据局将强化数据管理职责的综合性，将分散于中央网络安全和信息化委员会办公室、国家发展与改革委员会等多个部门的数据管理权限进行优化归并、汇聚整合，真正建立起标准统一、上下协同、运行高效的政府数据治理组织管理体系。

二是有利于权力运行的集约化。通过健全机构，规范分工，强化数据权力的垂直性配置与内部制约，实现数据开放共享、数据资产开发、数据安全管理、平台运营等多领域齐头并进，预计将进一步从纵向打通数据采集、加工、传递、再利用、存储等各环节管理，从横向上无缝衔接数据规划、数据质量等各业务切面，形成首尾相连、循环通畅的数据价值链管理闭环。

三是有利于资源配置的集聚化。与发改、财政、人社等综合管理部门侧重于资源分配有所不同，数据治理中的协调需要资源集中或再分配。充分的行政授权、相应的行政级别和人员编制、基础设施与数字化项目的必要投入将赋予国家层面数据管理机构应有的行政资源调配能力和政府影响力。https://www.secrss.com/articles/52595

2、周鸿祎：城市数字安全服务中心模式未来如何发展

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。

https://mp.weixin.qq.com/s/9ekOz9GNoV1Ax-5hH0-SXg

3、廖立澄：能源行业数据跨境与数据利用的平衡之法

在数据合规方面，主要是从四个领域去进行管理：**第一是制度和流程**；**第二是数据跨境**，因为数据跨境对于外企来说非常重要，但也是比较敏感、相对独立的领域；**第三是基础架构保护**；**第四是应用程序安全**。

总体来说，因为我们有覆盖制度流程、基础架构、应用程序的等级保护制度，**我们的合规工作主要集中于数据跨境和等级保护**。在数据跨境方面，从人、流程和技术这三方面，确保合规活动的落地。

首先，**从人的方面来说，应提高合规安全的意识**。具体涉及两个层面，**首先是“向上”，即我们必须让管理层知道合规很重要，并且去要获取他们的支持**。

其次是**从流程上**，涉及两个方面：**一方面是内部自评估流程**，即建立一套完善的表格，包含了对于发送方和接收方数据安全的控制能力，还有用于发送数据应用程序安全方面的控制能力评估，我们把全部内容放置在一个表格里去做评估，这就是自评估；**另外一个是申报**，即根据网信办等相关部门的流程去做申报。总体上，我们从自评估和申报内外两个流程，去做数据跨境合规工作。

最后一部分是技术。技术涉及到的内容比较多，举一个例子，我们去部署数据泄漏防护系统（DLP），该系统通过一些设置，除了保障组织内部到外部防泄漏外，还可以去监控数据跨境活动。比如，跨境到境外的供应商或者是加拿大总公司利用 DLP 等技术手段，可以更好地帮助我们掌握数据跨境的可见度。

https://www.secrss.com/articles/52705

4、张连起：锻造数据要素底层竞争力 助力建设科技强国

今年全国两会上，全国政协委员、中国税务学会副会长张连起带来了《关于锻造我国数据要素底层科技竞争力的提

案》。他认为，我国要发展成为数据强国，应在数据要素底层科技上加大投入，加快数据要素关键核心技术攻关，优化数据要素底层技术产业布局，从而争夺数据要素底层科技的制高点。

张连起认为，目前，该行业在三个方面仍存在一些问题，需要重点关注，一是**对于关键数据技术未来相关风险的研判和应对有待加强**；二是**新兴数据技术持续创新和迭代完善，有待持续“练兵”**；三是我国的数据要素市场体系仍在发展初期，**部分关键数据技术互联互通不足，规模化发展有待进一步提升**。

针对解决这些问题，张连起给出了以下三个方面的建议：

一是**要识别潜在“卡脖子”技术风险并转变为“攻坚”清单，确保关键数据技术自主可控**。张连起表示，要组织产业专家，系统梳理数据要素关键底层技术，识别潜在风险，制定并发布数据要素关键技术目录；同时，结合关键技术目录，鼓励科研机构和创新企业等科研力量产学研结合，充分发挥各方主动性和创造性，保障关键数据技术的自主可控。

二是**要加快建设数据基础制度先行先试区，通过产业应用试点牵引数据科技创新**。张连起认为，加快建设数据基础制度先行先试区，可先从公共数据开放利用等应用场景切入，为数据技术应用提供更多试点场景；此外，还要完善关键数

据技术的行业测评和安全认证机制，并对监管合规要求尚存模糊的新技术应用制定创新容错机制，鼓励企业参与产业应用试点，推动技术融合和自主可控产品的应用落地。

三是**要引导加强行业合作，增强数据技术的互联互通，为数据科技规模化发展创造条件**。张连起称，要支持科技企业牵头构建数据科技产业联盟，联合产业链上下游共同制定关键技术标准和产业落地最佳实践，促进产业各方在互联互通层面的协作。

此外，还要鼓励开源创新，以开源开放为抓手，推动数据科技产业规模化发展和技术创新。

http://lianghui.people.com.cn/2023/n1/2023/0307/c452473-32638871.html

5、雷军：完善行业数据安全管理体系

智能网联汽车作为车轮上的“数据中心”，其承载的行驶轨迹、生物特征等各类信息，既是数字经济发展的重要要素资产，也给个人隐私、国家公共利益与安全保障带来挑战。全国人大代表，小米集团董事长兼 CEO 雷军建议，加快制定围绕汽车生命周期和数据生命周期两条主线的数据安全标准指导产业发展，建立智能网联汽车数据安全认证制度、数据安全评级及公示制度，提升行业透明度与可信度。

“当前，各车企间数据尚未实现有效安全流通，数据孤岛普遍存在，数据价值无法充分发挥。”雷军代表建议，应当在保障数据安全的前提下，构建汽车数据共享机制及平台，让各车企数据实现流通。

雷军代表认为，在新能源汽车行业爆发式增长的今天，除了构建完善汽车行业数据安全管理体系，还要大力弘扬和发展汽车文化，提升汽车工业软实力。为此，可引导营造更加丰富的汽车文化场景，鼓励促进赛车运动、公路旅行、露营营地等文化场景的开发，与文旅产业发展相结合，形成“汽车技术/产品发展—汽车文化兴盛—汽车技术进步和消费需求持续提升”的正循环。

https://finance.sina.com.cn/jjxw/2023-03-12/doc-imykqmvx2167020.shtml

数据安全事件

1、航空公司 Safran Group 系统配置错误导致敏感数据泄露

据媒体 3 月 15 日报道，法国的跨国航空公司 Safran Group 系统配置错误导致敏感数据泄露。这是全球第八大航空航天供应商，2022 年的收入超过 190 亿欧元。研究人员发现，开源视频通话应用程序 Jitsi Meet 的测试版配置中使用了一个公开的环境文件。据估计，该文件已公开了一年半左右。泄露信息包括 Laravel 应用程序密钥、JSON Web 令牌(JWT)密钥、MySQL 凭据和 SMTP 凭据等，这些密钥和凭据可被攻击者用来访问网站后端、员工计算机和其它服务器。

https://cybernews.com/security/key-aerospace-player-leaks-sensitive-data/

2、Latitude Finance 遭到攻击泄露超过 30 万客户的信息

媒体 3 月 15 日称，金融贷款机构 Latitude Finance 遭到黑客攻击，超过 300000 份客户身份证明文件被盗。该公司表示，过去几天在其系统上检测到异常活动。在公司采取措施前，黑客窃取了员工的登录信息，以访问其它两家服务提供商持有的客户信息。其中第一家提供商泄露了约 103000 份身份证明文件，第二家提供商泄露了约 225000 条客户记录。

该公司表示，攻击源自该服务使用的一个供应商。

https://7news.com.au/business/retail/latitude-financial-hacked-as-300000-customer-identification-documents-stolen--c-10056836

3、美国 USMS 350GB 的执法信息以 15 万美元在黑客论坛出售

媒体 3 月 15 日报道称，美国法警局(USMS)的 350 GB 数据在一个俄语黑客论坛上出售。据卖家称，该数据库的售价为 150000 美元，其中包含 2021 年至 2023 年 2 月期间来自文件服务器和工作计算机的文件，不会像 exe 文件和库那样泛滥。这些信息包括军事基地和其它高度安全区域的航拍镜头和照片、护照和身份证件的复印件，以及窃听和监视公民的详细信息。还包含有关罪犯、帮派头目和贩毒集团的信息，部分文件被标记为机密或绝密。

https://www.bleepingcomputer.com/news/security/hacker-selling-data-allegedly-stolen-in-us-marshals-service-hack/

4、医疗保健提供商 ILS 透露超过 420 万患者的信息泄露

媒体 3 月 15 日称，医疗保健提供商 Independent Living

Systems(ILS)发布通知,透露数据泄露事件影响了 4226508 个患者。该公司发现其系统于 2022 年 7 月 5 日遭到攻击，随后调查显示攻击者在 2022 年 6 月 30 日至 7 月 5 日获得了部分 ILS 系统的访问权限。泄露信息涉及姓名、社会安全号码、纳税人识别号和医疗信息等。ILS 在发现违规行为后的六个月后，也就是 2023 年 1 月 17 日完成了确定受影响个人或实体的内部审查。最后，ILS 表示将为受影响患者提供为期一年的 Experian 身份保护服务。

https://www.databreaches.net/independent-living-systems-updates-its-breach-disclosure-notifying-more-than-4-2-million-patients/

5、9 亿份印度警方记录被盗，600G 数据在暗网出售

3 月 14 日，在某论坛上，一名用户声称拥有一个包含超过 9 亿份印度法律文件的数据库，其中包括印度警方记录、报告、法庭案件以及被告和被捕人员等详细信息。

据了解，该用户正在论坛上出售这些数据，文件总大小约为 600GB，数据格式为 JSON，并给出了原始 PDF 文件的链接。目前这些数据的真实性尚未确定，亦不清楚黑客究竟是如何获取到这些数据的。印度政府表态，立即采取行动调查此事，并采取必要的措施，防止出售这种敏感信息。

https://thecyberexpress.com/900-million-indian-police-records-stolen/

6、俄罗斯新冠疫苗 "机密"信息遭遇泄露

3 月 14 日，Cyber News 网站披露，黑客组织 KelvinSecurity 在网上共享了数百份文件，其中包含俄罗斯 Sputnik V 新冠肺炎疫苗开发的相关信息，其中一些文件甚至囊括了临床试验中已故参与者的姓名信息。披露的文件中包含了疫苗开发阶段、财务成本和技术细节相关的文件等机密信息。

https://cybernews.com/news/classified-documents-russian-sputnik-vaccine-online/

7、LockBit 勒索软件团伙窃取 SpaceX 3000 张设计图纸

近日，勒索软件组织 LockBit 给埃隆·马斯克（Elon Musk）发送了一条信息：打钱，或者眼睁睁看着 SpaceX 的机密信息在暗网上被卖掉。

根据网络安全分析师 Dominic Alvieri 上周三发布的推文，LockBit 勒索软件组织威胁要发布被盗的 SpaceX 设计图纸，除非埃隆·马斯克在 3 月 20 日前支付“保密费”。

据报道，这些机密图纸不是来自 SpaceX 本身，而是来

自其第三方供应商：为 SpaceX 项目生产零件的 Max Industries。LockBit 宣称入侵了 SpaceX 最大的零部件提供商 Max Industires，并窃取了 3000 张设计图纸。

https://www.secrss.com/articles/52821

8、美国医疗设备商 ZOLL 遭网络攻击，100 万人敏感信息被泄露

近日，医疗设备制造商 ZOLL 表示，1 月份的一次网络攻击暴露了超过 100 万人的敏感信息。ZOLL 表示事件始于 1 月 28 日，当时他们在其内部网络上“检测到异常活动”。该公司补充到，信息是在 2 月 2 日被访问的，对该事件的调查正在进行中。可能已泄露的信息包括您的姓名、地址、出生日期和社会安全号码。

https://www.secrss.com/articles/52811

9、加密货币交易所在线暴露敏感客户记录

3 月 15 日消息，一名网络安全研究员最近发现并报告了一个不受密码保护数据库，其中包含与加密货币销售平台相关的敏感记录，任何人都可以通过互联网连接访问这些数据。

经过进一步研究，发现该数据库属于 Fiatusdt.com，该公司提供了一个用于买卖加密货币的在线兑换货币平台。泄露

的数据记录包括了客户姓名、银行帐号、购买和销售记录等。由于加密货币投资者和交易者没有受到具体的监管规则或监督，这也意味着在加密货币的数据安全措施方面没有单独可用的行业标准。

https://www.websiteplanet.com/news/fiatusdt-leak-report/?&web_view=true

10、塔斯卡卢萨护理服务机构的数据泄露事件可能影响 82,000 名患者

3 月 15 日，据外媒报道，塔斯卡卢萨一家名为 NorthStar 的私人救护车服务机构的网络安全漏洞可能让不良行为者获得了 80,000 多名患者的记录。

经调查，NorthStar 了解到未经授权的行为者访问了存储在其网络上的某些数据。该公司表示，他们没有证据表明被访问的数据被滥用于其他网络犯罪或身份盗用，但受影响的数据包含极其敏感的个人信息，包括：姓名、社会保险号码、出生日期、患者 ID 号码、治疗信息、Medicare/Medicaid 编号和/或健康保险信息。

https://tuscaloosathread.com/data-breach-at-tuscaloosas-northstar-paramedic-services-could-impact-82000-patients/?&web_view=true

11、NBA 已承认！敏感数据泄露，警告球迷安全风险

3 月 18 日报道，据 bleeping computer 消息，美国国家篮球协会（NBA）公开承认，其在第三方提供商的部分球迷敏感数据已被泄露，提醒广大球迷防范可能发生的网络钓鱼攻击或诈骗。

NBA 拥有数量庞大的粉丝群体，在此次数据泄露事件中，尚未公布泄露的数据量和涉及影响范围。

据 NBA 发送的“网络安全事件通知”电子邮件称，“我们（NBA）最近发现，未经授权的第三方获得了您的姓名和电子邮件地址的访问权限，并获得了您的姓名和电子邮件地址的副本，这些信息由第三方服务提供商持有。没有迹象表明我们的系统、您的用户名、密码或您与我们共享的任何其他信息受到了影响。”

https://mp.weixin.qq.com/s/fOrRlZb25qWWlbDs9LEusw

《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/