全球数据安全观察

总第 138 期 2023 年第 19 期

(2023.06.12-2023.06.25)

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、浙江省网信办发布《浙江省个人信息出境标准合同备案指引》

6 月 14 日，浙江省互联网信息办公室发布了《浙江省个人信息出境标准合同备案指引》，以指导和帮助个人信息处理者规范、有序备案个人信息出境标准合同。指引中对适用范围、备案方式、备案流程等内容进行了规定。

https://mp.weixin.qq.com/s/W6IMepKUuNtUXvyZzPDNBQ

2、山东省网信办开通个人信息出境标准合同备案通道

6 月 14 日，山东省互联网信息办公室开通个人信息出境标准合同备案通道，对报送地址、备案材料提交邮箱及咨询电话进行公布，以指导和帮助全省个人信息处理者规范、有序备案个人信息出境标准合同。

https://mp.weixin.qq.com/s/A7vCHQKOTnqo1AXNpZZecw

3、新疆网信办：网络数据安全和个人信息保护专题举报通道正式开通

6 月 15 日，新疆维吾尔自治区互联网信息办公室开通网络数据安全和个人信息保护专题举报通道，明确了受理范围、

6 个方面的受理事项以及操作流程，规定该办公室即日起接受网络数据和个人信息违法违规行为监督举报线索。

https://mp.weixin.qq.com/s/JOKaEZek5cwZmwGiyv_HLA

4、北京市通过首家企业个人信息出境标准合同备案

近日，北京德亿信数据有限公司与香港诺华诚信有限公司签订的个人信息出境标准合同已通过市网信办组织的备案审核，备案号为“京合同备 202300001”，成为首家通过订立标准合同实现个人信息合规出境的企业，标志着个人信息出境标准合同备案制度在北京率先落地。

https://mp.weixin.qq.com/s/RNGmgfbMRjdZxDbv6eGdKQ

5、 “在线影音类”App 个人信息收集情况测试报告发布

6 月 12 日，中国网络空间安全协会、国家计算机网络应急技术处理协调中心对“在线影音类”公众大量使用的部分 App 收集个人信息情况进行测试的报告发布，本次测试选取了 19 家应用商店累计下载量达到 1 亿次的“在线影音类”App，共计 8 款。

http://www.cac.gov.cn/2023-06/12/c_1688218080926823.htm

6、英国和美国联合发布人工智能和数据传输合作大西洋宣言

6 月 8 日，英国和美国联合发布了《二十一世纪英美经济伙伴关系大西洋宣言》，要搭建两国间的数据桥梁，并在人工智能和隐私增强技术等方面进一步展开合作。英美数据桥是英国脱离欧盟后的首个独立数据桥，将促进英美之间个人数据的自由流动，推动跨大西洋研究和创新，为希望与跨大西洋合作伙伴协作和共享数据的组织提供更大的确定性。

https://www.dataguidance.com/news/international-uk-and-us-announce-atlantic-declaration

7、美国伊利诺伊州保险数据安全法案将生效

6 月 9 日，美国伊利诺伊州有关建立保险数据安全法的法案在两院获得通过后被送交州长签字，将于 2024 年 1 月 1 日生效。该法案旨在制定数据安全标准以及网络安全事件中主管机构的调查和通知标准，并适用于在该州获得许可的保险公司（被许可人）。法案规定，保险主管部门有权审查被许可人的任何事务，以查明被许可人是否曾经或正在从事任何违法行为。

https://www.dataguidance.com/news/illinois-bill-creation-insurance-data-security-law-sent

8、美国国家标准与技术研究院（NIST）宣布成立新的人工智能（AI）公共工作组

6 月 23 日，美国商务部宣布美国国家标准与技术研究院（NIST）将成立一个新的人工智能公共工作组，以应对快速发展的生成式人工智能的风险。

https://www.nist.gov/news-events/news/2023/06/biden-harris-administration-announces-new-nist-public-working-group-ai

9、欧洲议会通过人工智能法案草案，立法进入最终程序

6 月 14 日，欧洲议会全体会议表决通过了《人工智能法案》授权草案，该法案进入欧盟立法严格监管人工智能技术应用的最终谈判阶段。该法案草案的一个突出特点是注重基于风险来制定监管制度，以平衡人工智能的创新发展与安全规范。草案将人工智能风险分为不可接受的风险、高风险、有限的风险和极小的风险四级，对应不同的监管要求。

http://www.news.cn/tech/20230619/6491d4d375744437b6a63eb9d55474c8/c.html

技术、产品与市场

1、《2023 年公有云数据安全态势调查报告》发布

日前，以色列云数据安全公司 Laminar 发布了《2023 年公有云数据安全态势调查报告》，通过对近百位企业组织的安全管理和运维人员进行问卷调查和访谈，研究人员力求更深入了解当前公有云数据安全的风险态势和挑战。报告调研数据显示，39%的受访企业对现有的云上数据安全防护措施应用信心不足，越来越多的企业开始寻求云原生的安全解决方案，以获得跨多云环境的统一数据保护视图与策略，并实施符合纵深防御策略的安全控制。**报告关键发现如下：**

- **97%的受访企业已经设置了专门的数据安全人员或团队来处理公有云上数据安全问题**。这一比例同比 2022 年（58%）呈大幅上升趋势；
- 云上新的数据安全缺口正在快速出现，包括云应用配置错误或被弃用的云数据存储，攻击者们正在利用这些问题访问云服务并窃取数据。据 OWASP 研究人员测试，90%的云应用程序都不同程度存在了安全配置错误的问题；
- 调查数据显示，“人为因素”仍然是导致企业公有云上数据泄露和安全攻击的主要原因（占比 82%），主要包

括内部恶意人员、应用疏忽或操作错误等。每个人都会犯错误，因此企业需要借助完善的流程和先进的技术来加强防御。

https://mp.weixin.qq.com/s/mzJR4tpsD9x8MCgAAb1Ufg

2、最新报告：25%员工向 ChatGPT 等 AI 工具上传敏感数据

一项新的研究发现，15%的员工经常在 ChatGPT 上上传公司数据，其中超过四分之一的数据被认为是敏感信息，这使公司在无形中面临安全漏洞的风险。

6 月的研究报告《揭示真正的 GenAI 数据暴露风险》分析了超过 10000 名员工，主要研究员工如何在工作场景下使用 ChatGPT 和其他生成性 AI 应用程序。

该报告显示，至少有 15%的员工在工作中使用 ChatGPT 和其他生成性人工智能工具，其中近 25%的访问直接将公司数据粘贴在 AI 工具中。许多员工每周、甚至每天都在粘贴敏感数据。

根据报告显示，员工平均每天向生成性人工智能工具输入数据 36 次，而且随着人工智能的普及，这些数字预计只会增加。

https://www.freebuf.com/news/369694.html

3、IDC 2022 年中国工控安全审计市场份额报告正式发布

近年来，工业领域安全事件的不断频发、数字化转型大背景下 IT 与 OT 融合的持续加深，政策监管力度的不断增强都在驱动着中国工控安全市场的发展。其中，除了传统的网络安全技术外，工控防火墙、工控网闸、工控安全审计、工控安全管理平台等产品均迎来了市场的快速发展期。IDC 最新发布的《全球 OT 安全预测，2022-2026》报告显示，到 2026 年，全球工控安全市场规模将达到 67.6 亿美元，年复合增长率将达到 28.4%。

面对不断增长和变化的客户需求，IDC 给出如下建议，帮助技术提供商赢得市场：

工控安全审计产品的云化、虚拟化形态将快速发展来适应不断变化的用户需求。

工控安全审计将向智能化、自动化、可视化、协同化等方向发展：首先，除白名单的自学习外，审计产品的智能化、自动化可以帮助用户解决日志分析、日志管理的痛点。与此同时，审计的结果呈现至关重要，审计内容、报表的精细化、可视化对于最终用户具有重要价值。最后，审计产品需要和众多其他安全产品以及第三方平台、客户自有系统、平台的对接，从而进行统一管理。

行业化解决方案将帮助厂商和用户实现双赢：面对市场，

聚焦优势行业，推出适应行业要求的行业款型和解决方案对于技术提供商提高市场覆盖率具有关键作用，行业款型也可以更好地满足用户的场景化需求，从而实现用户与厂商的双赢。

https://mp.weixin.qq.com/s/64uA5b3bNj6xLw5C-SYnug

4、LockBit 勒索软件在美国行动 1700 次，共勒索 9100 万美元

在 LockBit 勒索软件联合咨询报告中，美国和国际网络安全机构表示，自 2020 年以来，该团伙对美国实体组织发动了约 1700 次攻击，成功勒索了约 9100 万美元。

LockBit 勒索软件即服务 (RaaS) 吸引附属公司使用 LockBit 进行勒索软件攻击，从而导致形成一个由互不相关的威胁行为者组成的大型网络，实施多种多样的攻击。

网络犯罪活动攻击了广泛的关键基础设施部门，包括金融服务、食品和农业、教育、能源、政府和紧急服务、医疗保健、制造和运输。

https://thehackernews.com/2023/06/lockbit-ransomware-extorts-91-million.html

5、2022 年中国数据治理市场份额发布

IDC 于近日发布了《中国数据治理市场份额，2022》报

告，追踪了数据治理市场进展。报告将该市场分为数据治理平台市场以及数据治理解决方案市场。

中国数据治理市场生态图谱，2023

数据治理平台级市场是指以治理平台为主要产品，与生态伙伴合作提供解决方案的厂商构成的市场。相比 2021 年，市场规模增长了 12.6%。阿里云保持高速增长并遥遥领先，其次为中国电子、数梦工场。在当前追踪的厂商之外，华为云、腾讯云等也开始重点发力平台市场；成长型大数据企业如滴普科技、科杰科技等在其大数据套件中也提供专业的数据治理开发工具，未来 1 年都有望占据一定的市场份额。

数据治理解决方案市场是指依托数据治理工具为用户提供数据治理方案的厂商构成的市场。相比 2021 年，该市场增长了 7.4%。亿信华辰、百分点仍然保持领先位置，其次是数梦工场、四方伟业。此外，在竞争最为激烈的数字政府领

域、金融领域，以及能源等行业，也有大量行业解决方案商提供细分场景的数据治理服务。

https://mp.weixin.qq.com/s/dyOaggwQuZaGW-CeUpglIw

业界观点

1、网信办：切实维护网络安全，增强数据安全保障能力

5 月 23 日，国家互联网信息办公室发布《数字中国发展报告(2022 年)》 ，并展望 2023 年数字中国发展工作。

报告显示，2022 年数字中国建设取得显著成效。数字基础设施规模能级大幅提升。报告提到，数字经济成为稳增长促转型的重要引擎。

展望 2023 年，报告明确四个方面加快建设数字中国。

一是夯实数字中国建设基础。

二是全面赋能经济社会发展。

三是强化数字中国关键能力。构筑自立自强的数字技术创新体系，加快推进数字领域关键核心技术突破，强化企业科技创新主体地位，发挥科技型骨干企业引领支撑作用。**筑牢可信可控的数字安全屏障，切实维护网络安全，增强数据安全保障能力，提升个人信息保护水平**。

四是优化数字化发展环境。

https://www.chinanews.com.cn/cj/2023/05-23/10012463.shtml

2、人民日报：筑牢数字安全屏障

今年2月，中共中央、国务院印发《数字中国建设整体布局规划》，提出“筑牢可信可控的数字安全屏障”。数据显示，2022年，我国数字经济规模达到50.2万亿元，总量稳居世界第二。数字经济蓬勃发展的同时，数字安全问题不容小觑。非法获取个人信息、网络诈骗等违法犯罪活动，侵害个人财产和隐私安全；网络攻击、网络窃密等行为，给社会治理、国家安全带来挑战。

专家介绍，数字安全是指保护计算机系统、网络及其数据的机密性、完整性和可用性，以及防止未经授权的访问、窃取、破坏、篡改和泄露。数字安全涵盖了多个方面，包括计算机安全、网络安全、移动设备安全、数据安全等等。科学平衡数据安全保护和数据有序流动之间的关系，是发展数字经济的重要前提。

中国发展研究基金会副理事长刘世锦认为，把握好数字经济发展和数字安全的关系，应坚持“用”字当头。“既要重视数据产权保护不力、数据不安全等问题，也要坚持用足用好各类数据资源，在数据产权保护和安全上守住底线。”刘世锦说。

数据是一种新型生产要素，具有非竞争性、无限供给、易复制、边际成本极低等属性。在中国工程院院士方滨兴看来，当前，数据使用权和所有权分离、数据可用不可见、数据不动程序动、分享价值不分享数据等新的数据安全理念，有助于破解数据要素流动与隐私保护之间的矛盾。

方滨兴说，以可信计算为例，“数据不动程序动”指的是把数据集中在固定的可信计算平台上,在对数据进行价值“挖掘”时，在可信计算平台上运行程序，最终只能将结果带走，个人数据等仍存留在平台上。数据使用权交易时则强调“可用不可见”——数据共享汇聚到可信计算平台后再进行数据交易，平台交易的是数据使用权，而不是所有权。

人工智能的发展，激发数字安全应用潜力。国家信息中心党委专职副书记吴文化表示，从发展机遇看，人工智能给数字安全带来了三个转变：一是网络安全防御由被动变主动，有助于提升网络安全防御能力；二是网络安全运维从高成本变高效率，有助于提高网络安全运维的整体保障水平；三是网络安全人才由长周期培养变短时间胜任，有助于缓解人才短缺问题。

当前，数字安全的理念、体系、技术等也在逐步发生新变化。杭州安恒信息技术股份有限公司董事长范渊认为，在产业数字化过程中，数字安全要实现政府、社会、企业等多

方面协同，筑牢数字安全屏障，在考虑产品功能同时，也要重视数字安全的能力建设。

http://data.people.com.cn/rmrb/20230619/19/f896b5a169e44a7c83795a3d5dee7b1a_print.html

3、张峰等：人工智能安全风险分析及应对策略

以 ChatGPT 为代表的生成式人工智能技术在网络安全领域是一把“双刃剑”，一方面，ChatGPT 可以赋能网络安全，提升风险检测与防护能力；另一方面，ChatGPT 技术的滥用将对国家、社会、公众带来负面影响，同时，AI 新技术的脆弱性也使得 ChatGPT 应用自身面临安全风险。

（一）人工智能技术滥用带来的安全风险

存在国家政治军事风险。第一，存在由于民族或政治偏见带来的严重不公平问题。第二，基于用户画像进行情报收集和影响政治主张。第三，辅助军事决策并应用于军事打击。

存在不良信息传播风险。一方面因 AI 应用内容过滤机制不完善造成不良信息传输。另一方面，AI 产生不良信息内容易误导或诱导用户。

存在网络攻击利用风险。一是 AI 帮助黑客提高网络攻击方面的技术知识与能力。二是攻击者利用 AI 编程能力来生成网络攻击工具。三是 AI 基于社会工程学知识生成网络

钓鱼等信息。

（二）人工智能应用自身面临的安全风险

一是存在数据安全风险。用户在使用 ChatGPT 等 AI 应用时可能不自觉输入个人隐私数据，这些数据经过训练可构建出用户画像。AI 平台收集的原始数据与衍生数据的归属权、控制权与使用权等问题目前在法律上还是很难界定。即使用户要求删除，也很难保证其会主动实施擦除操作，存在个人隐私信息泄露风险。

二是存在算法安全风险。一方面存在算法被欺骗攻击风险。另一方面，存在 AI 数据投毒攻击风险。

三是存在平台及供应链安全风险。ChatGPT 等 AI 平台系统仍存在通用的网络安全风险，如算法后门嵌入、代码安全漏洞等。

（三）人工智能应用伴生的社会伦理风险

一是引发 AI 替人的失业恐慌情绪。二是引发 AI 生成内容知识产权问题。三是影响正常社会秩序。

对此提出了四个方面的相关建议:

（一）国家层面: 健全人工智能安全政策法规，强化 AI 滥用法律约束

一是依据相关国家顶层规划制定人工智能安全相关国家战略。二是布局人工智能法规体系，应覆盖道德伦理、人

身安全、个人隐私保护、算法规范应用、防范技术滥用和知识产生等方面。三是推动现有法律法规向人工智能领域延伸适用。四是强化 AI 滥用法律约束。

（二）产业层面：重点关注 AI 技术自主可控及算力网络赋能 AI 大模型发展

一是提升软硬件实力，实现高端芯片与 AI 框架自主可控。二是算力网络赋能 AI 大模型发展。

（三）行业层面：倡导 AI 技术合规使用和加强行业自律

一是建立行业监管制度并开展合规性评估审查。二是创新研究应用人工智能赋能网络安全技术。一方面，利用 AI 技术赋能针对复杂网络攻击的防御能力，使用 AI 技术应对其带来的网络安全风险；另一方面，研究利用 AI 技术提升企业组织在网络安全攻击检测、数据资产识别与风险监测、业务安全风控、不良信息识别、电信反诈、安全威胁分析、深度伪造识别等方面的能力。三是做好元宇宙等 AI 融合场景的安全风险梳理与防护技术储备。

（四）企业层面：加强 AI 安全防护体系建设，保障 AI 业务健康安全运行

一是制定出台企业组织 AI 安全总体策略，编制企业标准规范与技术指南；二是配备 AI 安全领域专业人员，支撑

AI 安全新技术新业务安全风险评估与创新技术研究；三是对员工在日常工作或对外服务中使用 ChatGPT 等 AI 应用行为进行规范，防范企业组织及客户数据泄露等风险；四是强化安全技术手段建设，建设涵盖网络安全、算法安全、数据安全与隐私保护等功能的 AI 安全管控能力，为企业组织的 AI 能力与应用提供安全防护，保障 AI 业务健康发展。

（五）公众层面：强化人工智能技术滥用防范意识，保障自身权益

一是强化安全宣传。二是提升防范意识。

https://mp.weixin.qq.com/s/HF6rcp0-11LIVrsNKzzUfQ

4、魏婷婷：完善数据合规监管需实现“四个转变”

为避免数据合规监管失灵，合规监管的思路也必须及时作出调整，通过四个方面的转变积极推动数据合规监管实现“从有到优”的修正完善。

首先，监管立法思路从硬法约束转向“硬法与软法”并重。

其次，监管主体从单一政府主导迈向政府、企业与行业多元主体协同。

再次，监管理念从严格的合规监管过渡到包容审慎的合规监管。

最后，监管策略从以“获得数据权利人事前同意”为核心，

转到以“数据利用与再利用”为核心。

https://mp.weixin.qq.com/s/32gz-5QTz1g5PwJ22Zp9Xw

5、徐展：加强数字安全免疫力，促进数字化时代韧性发展

6 月 17 日，第三届数字安全大会在北京召开。腾讯安全数据安全商业化总监徐展以《加强数字安全免疫力，促进数字化时代韧性发展》为主题分享，指出数据安全已成为企业发展的关键。面临的挑战包括：数据安全建设滞后于数字化进程；数据隐私和合规压力增加；企业的暗数据增多，导致数据泄露；新的数据威胁，如 API 泄露，身份攻击和勒索攻击；以及企业对数据泄露的反应迟缓。

为应对这些挑战，徐展表示腾讯安全提出一个数据安全免疫力框架，包括四个方面：

一、数据默认安全：将数据安全和整体安全建设视为一体，从业务建设初期就考虑数据全生命周期的安全防护。

二、数据看得见：能看到并跟踪数据在企业内部的流转，给数据打上标签，使其流向可追踪。

三、数据保护、防御能力：构建能管控风险并能处置的数据安全体系。

四、数据安全智能化运营，风险闭环：通过 DataSecOps 数据安全运营体系，做风险闭环，做持续的检查、核查，不

断完善风险能力。

根据不同的业务场景，采取相应的安全免疫力建设方式，包括数据防泄漏、加密、零信任、数据分类识别、脱敏等策略。同时，也要建立数据治理的框架，对数据安全进行评估和风险排查，贯穿数据安全建设的每一个流程，并保证数据安全建设的方法的有效性。

https://www.sohu.com/a/687924988_121035526

数据安全事件

1、被罚百万！为政府部门开发系统造成数据泄露

根据“公安部网安局”微信公众号发布的消息，2023 年 3 月，浙江温州公安网安部门在查处一起涉数据安全违法案件时发现问题。

浙江某科技有限公司为浙江某县级市政府部门开发运维信息管理系统的过程中，在未经建设单位同意的情况下，将建设单位采集的敏感业务数据擅自上传至租用的公有云服务器上，且未采取安全保护措施，造成了严重的数据泄露。

浙江温州公安机关根据《中华人民共和国数据安全法》第四十五条的规定，对公司及项目主管人员、直接责任人员分别作出罚款 100 万元、8 万元、6 万元的行政处罚。

https://www.freebuf.com/news/369775.html

2、因多次索要个人权限和信息，星巴克被上海网信办约谈

6 月中旬，国内某新闻媒体披露上海商圈中一家星巴克点餐小程序过度索客户信息，仅是点 1 杯咖啡，消费者至少被弹窗提示注册会员 3 次，弹窗索要定位授权 2 次。对此，上海市网信办、市市场监管局共执法人员来到位于星巴克涉事门店，向该店工作人员指出上述问题涉嫌违反《个人信息保护法》的有关要求，已要求门店方向其公司高层及时反馈，按时参加约谈，并将指导相关企业进一步整改。

https://www.freebuf.com/news/369936.html

3、BlackCat 勒索软件声称从 Reddit 窃取了 80GB 的数据

据 Security Affairs 6 月 18 日消息，曾于今年 2 月 5 日攻击流行社交新闻聚合平台 Reddit 的幕后主使于近日浮出水面，BlackCat(又名 ALPHV)勒索软件组织发布消息称对这起网络攻击负责。

Reddit 曾在事发后表示，该攻击是针对对 Reddit 员工的一次复杂网络钓鱼活动，将他们引导至一个假冒的公司内网网关站点，骗取其账号和密码，进而获得一些内部文档和业务系统的访问权限。Reddit 曾指出有部分公司员工及广告

商信息被泄露，Reddit 用户密码和账户没有受到损害。

但如今 BlackCat 宣布他们窃取了 Reddit 80GB 的数据压缩包，并表示 Reddit 没有查明所有被窃取的数据类型。在给 Reddit 的最后一封电子邮件中，BlackCat 提出了 450 万美元的赎金需求，并要求 Reddit 撤回对第三方应用收费的决议，否则将泄露这些数据。

https://www.freebuf.com/news/369913.html

4、Rhysida 勒索软件泄露了从智利军队窃取的文件

6 月 15 日，据外媒报道，名为 Rhysida 的勒索软件行动背后的威胁参与者已经在网上泄露了他们声称是从智利军队 (Ej é rcito de Chile) 网络中窃取的文件。

漏洞发生后，网络被隔离，军事安全专家开始了受影响系统的恢复过程。攻击事件曝光几天后，当地媒体报道称，一名陆军下士因参与勒索软件攻击而被捕并受到指控。

CronUp 安全研究员表示，Rhysida 勒索软件发布了大约 360,000 份智利陆军文件（据他们称，这一比例仅为 30%）。

https://www.bleepingcomputer.com/news/security/rhysida-ransomware-leaks-documents-stolen-from-chilean-army/

5、调查发现超 10 万名 ChatGPT 用户信息被黑客出售

6 月 21 日报道，根据国际网络安全公司 Group-IB 的报告，超过 10 万名 ChatGPT 用户的个人信息被泄露，有黑客正在暗网交易平台进行出售。

Group-IB 深入调查暗网数据，统计了在 2022 年 6 月至今年 5 月之间暗网发现的 ChatGPT 用户信息，发现今年 5 月达到峰值，出售 26802 条 ChatGPT 用户信息。

按照国家来划分大部分数据来自印度（12632 条记录），巴基斯坦（9217 条记录）和巴西（6531 条记录），来自越南、埃及、美国、法国、摩洛哥、印度尼西亚和孟加拉国的聊天机器人用户的数据也出现在暗网上。

分析还显示，大多数记录（78348 条记录）都是使用 Raccon 恶意软件窃取作为恶意软件即服务提供的信息而被盗的，其次是 Windows 间谍软件和隐形工具 Vidar。

http://www.techweb.com.cn/it/2023-06-21/2929080.shtml

6、厦门一公司系统被攻击，超百万条用户信息泄露且遭黑产滥用

黑客团伙攻击厦门一科技公司系统，非法获取公民个人信息百万余条并出售，非法获利约 40 万元。

近期，厦门市公安局网安支队联合思明分局横跨 4 省市，

成功打掉一个集黑客攻击、数据清洗、买卖信息、提供资金、数据使用等为一体的全链条网络犯罪团伙，破获某公司被侵犯公民个人信息案，抓获犯罪嫌疑人 7 名，查获非法获取的公民个人信息 100 万余条。

https://www.secrss.com/articles/55915

7、大量飞行员敏感数据泄露，全球最大航空公司遭遇供应链攻击

6 月 24 日消息，全球最大的两家航空公司美国航空和西南航空周五披露了因 Pilot Credentials 遭到黑客攻击而导致的数据泄露事件。Pilot Credentials 是一家管理多家航空公司飞行员申请和招聘门户的第三方供应商。

据报道，一名未经授权的个人于 4 月 30 日访问了飞行员证书系统，并窃取了包含某些申请人在飞行员和学员招聘过程中提供的信息的文件。两家航空公司均于 5 月 3 日获悉该泄露事件，并表示该事件影响范围仅限于第三方供应商的系统，不会对航空公司自己的网络或系统造成损害。

根据周五向缅因州总检察长办公室提交的泄露通知，美国航空表示，该数据泄露事件影响了 5745 名飞行员和申请者，而西南航空报告称，总共有 3009 名飞行员和申请者受到影响，泄露数据包括姓名、社会安全号码、驾驶执照号码、

护照号码、出生日期、飞行员证书号码等。

https://www.bleepingcomputer.com/news/security/american-airlines-southwest-airlines-disclose-data-breaches-affecting-pilots/

8、曼彻斯特大学遭遇网络攻击，并已确认数据被盗

6 月 23 日，据外媒报道，曼彻斯特大学最终证实，6 月初披露的网络攻击背后的攻击者窃取了校友和在校学生的数据。

据调查，此次攻击背后的黑客向学生发送了电子邮件，声称窃取了属于学生和教职员工的 7 TB 机密数据，包括学生和教职员工的机密个人信息、研究数据、医疗数据、警方报告、药检结果、数据库、人力资源文件、财务文件等等。

曼彻斯特大学现已证实，事件中用于帮助管理学生大学住宿的系统的数据确实被盗。根据网络攻击信息页面的更新，攻击者访问了以下类型的敏感数据: 姓名、地址、电话号码、电子邮件地址、大学 ID 号、出生日期和性别、国籍、住所和民族等等。

https://www.bleepingcomputer.com/news/security/university-of-manchester-confirms-data-theft-in-recent-cyberattack/

9、美国的 RateForce 网站约 93 GB 的超过 25 万条记录泄露

6 月 22 日，据报道，美国汽车保险比价网站 RateForce 泄露了大量用户 PII 信息。总共泄露了 96175 个文件夹，其中包含 255756 条记录，总大小为 93.93GB。此次泄露事件持续了至少两周，源于一个不安全的数据库，涉及各种文件的扫描件和图片，包括车辆登记、驾驶执照、保险卡和车辆所有权等。进一步调查发现，数据库中保单的主要保险公司是 USA Underwriters。

USA Underwriters 澄清道，他们聘请了独立的 IT 公司来管理其基础设施，并且不承担管理暴露的数据库的任何责任。目前，数据库已被保护起来。

https://www.hackread.com/rateforce-auto-insurance-data-leak/

10、PBI 数据泄露涉及 Genworth 和 CalPERS 数百万客户的信息

6 月 23 日，据报道，第三方供应商 PBI Research Services 的数据泄露事件影响了其三个合作公司的约 475 万客户。

这些攻击始于 5 月 27 日，当时 Clop 团伙开始利用 MOVEit Transfer 漏洞窃取组织的数据。第一家受影响组织是位于弗吉尼亚州的人寿保险服务提供商 Genworth Financial，据估计影响了 250 至 270 万人。第二家受到 PBI 泄露影响的

是位于纽约的保险提供商 Wilton Reassurance，涉及 1482490 名客户。受到影响的第三家公司是美国最大的公共养老基金 CalPERS（加州公共雇员退休系统），影响了约 769000 名会员。

https://www.bleepingcomputer.com/news/security/moveit-breach-impacts-genworth-calpers-as-data-for-32-million-exposed/

11、220 万个与英国 100 所顶尖大学相关的凭证在暗网上泄露

6 月 19 日，据报道，Crossword 在暗网上发现了近 220 万个与英国 100 所顶尖大学相关的凭证，其中 57%属于 24 所罗素集团大学。大学的位置和规模对泄露的程度也有影响，伦敦的风险要大得多，有 506330(20%)个证书被泄露，其次是东南部(334251，占比 13%)和苏格兰(306873，12%)。

研究人员还透露，超过一半（54%）的泄露来自拥有研究设施的英国大学，政府资助的核能和国防等领域的项目可能面临风险。

https://www.infosecurity-magazine.com/news/millions-uk-university-credentials/

12、美国路易斯安那州和俄勒冈州数百万居民的信息泄露

6 月 16 日报道称，路易斯安那州和俄勒冈州的 MOVEit Transfer 安全文件传输系统遭到攻击，数百万居民的信息泄露。路易斯安那州机动车辆办公室(OMV)透露，可能所有拥有该州政府颁发的驾驶执照、身份证或汽车登记证的居民都受到了影响。俄勒冈 DMV 也发布了类似的声明，称此次数据泄露事件影响了大约 3500000 名俄勒冈人。俄勒冈州当局表示，他们无法确定具体的受影响个人，因此建议所有公民采取预防措施。

https://www.bleepingcomputer.com/news/security/millions-of-oregon-louisiana-state-ids-stolen-in-moveit-breach/

13、FTC 指控基因检测公司 1health.io 泄露用户的健康信息

6 月 16 日，据报道，美国 FTC 指控基因健康检测公司 1health.io 未能保护敏感的基因和健康信息。FTC 称，1health 以前称为 Vitagene，在其隐私政策方面欺骗了客户，追溯性地更改了该政策，并在其删除数据的过程中误导了客户。该公司被要求向 FTC 支付 75000 美元用于消费者退款，并被禁止在未获得客户明确同意的情况下与第三方共享健康数据，还必须实施新的安全计划。1health 的首席执行官称 FTC 的调查是“政府过度干预的案例”。

https://cyberscoop.com/ftc-1healthio-health-data-privacy/

《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