全球数据安全观察

总第 90 期 2022 年第 18 期

（2022.05.23-2022.05.29）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、国家发改委牵头制定数据要素基础制度文件

5 月 17 日，全国政协在京召开专题协商会，围绕“推动数字经济持续健康发展”进行协商议政。对于全国政协委员在会议上的建议，国家发展改革委副主任林念修从四方面作了简要回应。

关于超前部署新型基础设施，夯实数字经济发展基础的问题。目前发改委正在牵头加快推进新型基础设施建设，部署全国一体化大数据中心体系，实施“东数西算”工程。下一步，将重点推进两方面工作。一方面，强化统筹布局。引导大型、超大型数据中心向国家算力枢纽节点集聚，形成国家数据中心集群。加快推进国家枢纽节点间的直联网络建设，促进东西部算力高效互补和协同联动。另一方面，坚持绿色发展。强化能源布局联动，提升绿色能源使用比例，着力建设绿色节能数据中心。

关于深度挖掘数字要素价值，拓展数字经济发展空间的问题。按照中央部署，发改委正在牵头制定数据要素基础制度文件。下一步，将加快推动文件出台，着力建设四方面制度。一是建立保障权益激活价值的数据产权制度。二是建立合规高效、场内外结合的数据要素流通交易制度。三是建立

体现效率、促进公平的数据要素收益分配制度。四是建立安全可控、弹性包容的数据要素安全治理制度。

关于加快数字化转型，推动实体经济高质量发展的问题。去年，发改委牵头起草并报请国务院印发了《“十四五”数字经济发展规划》，明确了“十四五”时期推动数字经济发展的蓝图。下一步，将围绕规划落实，重点推动三方面工作。一是研究起草推动数字化转型的指导意见。二是组织专项工程，提升行业整体数字化水平。三是布局数字化转型促进中心，提供数字化转型公共服务。

https://mp.weixin.qq.com/s/IuzZ_b0_8HAsJmy-stbyog

2、《河北省数字经济促进条例》正式发布，加强数据资源开发利用

5 月 27 日，《河北省数字经济促进条例》由河北省十三届人大常委会第三十次会议通过，将于 2022 年 7 月 1 日起施行。

这是全国第四部省级层面的数字经济促进条例，该条例对于贯彻落实党中央和省委关于发展数字经济的重大决策部署，规范有关部门管理职能，加快推进数字产业化、产业数字化，打造我省数字经济新优势，推动经济社会高质量发展具有重要意义。

《条例》共九章八十一条。围绕数字基础设施建设、数据资源开发利用、数字产业化、产业数字化、数字化治理、京津冀数字经济协同发展、保障和监督等方面作出规范。

首次专设京津冀数字经济协同发展一章，是条例一大亮点。探索破解“信息孤岛”“数据烟囱”，条例规定新建政务服务信息系统应当依托一体化政务服务平台进行建设，不得单独建设；明确一数一源、标准统一，不得重复收集、多头收集的数据收集原则；明确建立健全公共数据共享协调推进机制，对公共数据共享、数据回流以及公共数据开放进行规范。

加强数字化治理，推动数字政府建设，可提高政府科学决策、高效监管、精准治理水平。强化数字监管，条例加强全省一体化政务服务平台、一体化信用平台、一体化在线监管平台对接，推动政务服务数据、信用数据、执法监管数据跨部门、跨层级共享应用。同时，推进非现场监管、信用监管、风险预警等监管模式，提高监管效能和水平。

https://mp.weixin.qq.com/s/MRR8K0qkT4r6zuylyjsdng

3、上海立法核验个人健康信息，因防疫采集的个人信息不得泄露

5 月 24 日，上海市十五届人大常委会第四十次会议表决

通过了《上海市人民代表大会常务委员会关于进一步促进和保障城市运行“一网统管”建设的决定》（以下简称“《决定》“）。《决定》作为上海治理数字化领域的综合性决定，共 23 条，主要涵盖以下五方面内容：一是明确“一网统管”建设目标。二是明确“一网统管”运行体系。三是数据赋能基层治理。四是发挥治理数字化功能，规范推进疫情防控相关应用场景。五是加强“一网统管”建设保障。《决定》明确，上海运用治理数字化功能，在疫情防控期间，实行个人疫情防控信息核验措施（即“场所码”或“数字哨兵”等核验措施），核验个人健康信息。《决定》规定，出入公共场所、居民小区等场所的人员应当按照规定主动接受个人疫情防控信息核验。信息核验中采集、处理个人疫情防控信息应当遵守个人信息保护相关法律、法规的规定，采集的个人信息仅用于疫情防控需求，任何单位和个人不得泄露。实行个人疫情防控信息核验措施的具体办法，由上海市人民政府另行制定。

https://mp.weixin.qq.com/s/nvYDg0DZcSJzOEsfFaWelw

4、《黑龙江省促进大数据发展应用条例》发布

5 月 13 日，黑龙江省十三届人大常委会第三十三次会议通过了《黑龙江省促进大数据发展应用条例》（以下简称“条

例”），自 2022 年 7 月 1 日起施行。该条例是黑龙江省大数据领域的一部基础性地方法规，对运用法治方式贯彻落实国家大数据战略以及省委的相关决策部署、切实发挥数据作为生产要素的基础性资源作用和创新引擎功能，具有重要意义。条例共 8 章 70 条，紧贴龙江实际，保障数字化改革，深化数字龙江建设，推进龙江治理体系和治理能力现代化，重点在数据资源、培育数据要素市场、数据政策导向和促进措施等方面作出规定，形成一系列创新亮点。

条例完善了公共数据管理机制，对公共数据平台建设、公共数据目录管理、公共数据标准、公共数据的采集和汇聚、公共数据质量管控、公共数据开放等作出规定，从法规层面强化公共数据平台支撑能力，提高公共数据质量，优化公共数据要素资源配置。

条例对“数据要素市场”从建立数据交易平台、培育数据要素市场主体、促进数据高效流通、探索建立数据生产要素统计核算制度、数据质量评估认证、构建数据资产定价指标体系、数据管理主体责任以及公平竞争等 8 个方面作出明确规定，为充分发挥数据作为生产要素的基础性资源作用和创新引擎功能，培育壮大我省数据要素市场提供制度保障。

https://mp.weixin.qq.com/s/NGMEQYLL6KR7zPjKYmvksg

5、俄通过《保护关键信息基础设施国家政策基本原则》草案

据塔斯社 5 月 20 日报道，俄罗斯联邦安全委员会会议通过《保护关键信息基础设施国家政策基本原则》草案，并决定额外制定旨在改善俄罗斯信息安全体系的若干战略规划文件。

该草案定义了在信息技术部门实施国家政策的目的和机制，特别是计划通过使用国产信息技术提高关键信息基础设施的安全水平。草案决定运用国家力量组织研发人工智能、量子计算技术，创建富有竞争力的电子元件基地和高科技生产区，并开发用于检测、预防和消除网络攻击后果的国家信息系统。此外，草案还将特别关注信息安全领域的专家及技能培训。

对于该草案，俄罗斯总统普京提出三大关键任务：一是不断完善、调整与国防能力、经济和社会稳定发展直接相关的关键设施领域的信息安全保障机制；二是提高国家机构信息系统和通信网络的安全性，要加强对国内数字空间的防御，通过控制设备、通信等手段，降低公民信息和个人数据泄露风险；三是从根本上降低采用国外程序、计算机技术和电信设备相关风险，向国产设备、技术、方案和产品过渡。

https://mp.weixin.qq.com/s/UrUeG6CNYayhrs2xzTYkpA

技术、产品与市场

1、2022 数据泄露调查报告：勒索软件激增 13% 超过去 5 年总和

据 Verizon 发布的 Verizon Business 2022 数据泄露调查报告显示，勒索软件在 2022 年同比增长 13%，增幅超过过去五年的总和。Verizon 的研究表明，随着犯罪分子希望利用越来越复杂的恶意软件形式，勒索软件继续证明在利用非法访问私人信息并将其货币化方面特别成功。经济利益仍然是攻击的主要动机，其次是间谍活动。

该研究还表明，数据泄露的四个关键途径是未经授权的凭据、网络钓鱼、漏洞利用和僵尸网络。大约五分之四的违规行为可归因于有组织的犯罪，外部行为者造成组织违规的可能性是内部行为者的四倍。

https://www.verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf

2、2022 数博会：大数据产业规模突破 1.3 万亿

5 月 26 日，2022 中国国际大数据产业博览会启动线上开幕。本届数博会主题为“抢数字新机 享数字价值”，将举办“开幕式、数谷论坛、数博发布”等线上活动。

当前中央网信办正在积极推动数字中国整体布局，将以数据资源为核心，以数字基础设施为支撑，以数字技术为驱动，以数字治理和数字安全为保障，将数字化发展全面融入“五位一体”总体布局，推动建设高质量的数字经济，高效协同的数字政府，自信繁荣的数字文化，普惠包容的数字社会，绿色智慧的数字生态文明，以体制机制改革整体驱动生产、生活、治理方式数字化变革。

具体来看大数据产业，据工信部部长肖亚庆在开幕式上介绍，“十三五”时期我国大数据产业年均复合增长率超过30%，2021 年产业规模突破了 1.3 万亿元，大数据产业链初步形成。

https://www.163.com/dy/article/H8AF94DT05199NPP.html

3、机密计算时代或将很快到来

早在 2020 年，研究机构 Gartner 就在其年度云安全技术成熟度曲线中，将机密计算列为 33 种关键安全技术之一。但是 Gartner 曾经认为，机密计算需要较长时间的理论研究与研发准备，距离成熟的商业市场应用，还需要 5 到 10 年的时间。不过由于行业对数据安全在使用过程中的保护需求快速增长，机密计算的应用步伐有望大大加快。有研究机构预测，机密计算技术在未来 1~2 年内就会成为安全计算的标准

方法，尤其是在云计算环境中。

在企业应用需求和技术应用价值的双重推动下，机密计算概念的市场发展比预期要快很多。目前许多科技巨头纷纷入局，大力探索和开发机密计算。机密计算的产业生态也在不断完善。包括阿里巴巴、华为、AMD、微软、甲骨文、Google 等科技巨头公司在内的企业，已在 Linux 基金会下启动成立了机密计算技术应用联盟，旨在进一步加快技术应用标准的定义和开源工具的开发。

随着机密计算的应用加速，企业组织现阶段已经能够得益于这项技术的应用。研究机构建议企业应尽快探索机密计算技术的使用，特别是对于在云环境上部署应用系统和数据的企业。虽然目前机密计算在产品功能方面尚不完善，但基于现有技术的部署已经可以将数据安全性在原有基础上向前推进一大步。

https://mp.weixin.qq.com/s/VWOWdMLFC_j2l7UKGtTRtA

4、电子邮件依然是数据安全最大威胁

根据 Ponemon Institute 的最新研究报告，在过去 12 个月中，近 60% 的企业和机构经历过由于员工在电子邮件中犯下错误导致的数据丢失或泄露。

65% 的受访 IT 安全从业人员认为，电子邮件依然是组

织中数据丢失风险最高的渠道。紧随其后的是云文件共享服务（62%）和即时通讯平台（57%）。

该研究调查了全球 614 名 IT 安全从业人员，其他亮点数据还包括:

（1）由于不遵守政策而导致的员工疏忽是数据丢失事件的主要原因（40%）。

（2）27% 的数据丢失事件是由恶意内部人员造成的。

（3）安全和风险管理团队最多需要三天的时间来检测和修复由电子邮件中的恶意内部人员造成的数据丢失和泄露事件。

（4）23% 的组织每月遇到多达 30 起涉及员工使用电子邮件的安全事件（例如，电子邮件被发送给了非预期的收件人）。

https://www.wangan.com/p/7fy7f6408a63acc2

5、Meta 公司更新隐私政策，让用户更容易了解用户数据如何被使用

Facebook、WhatsApp 和 Instagram 的母公司 Meta 宣布，其隐私政策将有一系列新变化。据 Meta 公司称，这些变化旨在更清楚地向用户传达该公司如何使用其收集的信息。

Meta 公司强调，更新后的隐私政策并没有为该公司带来

任何收集、使用或分享用户数据的新方式。相反，它只是简化了措辞，并对政策和其他数据做法提供了更详细和更清晰的解释。新的隐私政策以前被称为数据政策，将于 7 月 26 日生效。这项政策涵盖 Facebook、Messenger、Instagram 和其他 Meta 产品。然而，WhatsApp、Workplace、Free Basics 和 Messenger Kids 并不包括在内。该公司也已经开始向用户发送关于新政策的通知。用户可以点击通知，查看变化并阅读更多细节。

https://www.cnbeta.com/articles/tech/1274499.htm

业界观点

1、谢玮：《数据安全法》使数据安全管理步入新阶段

近日，在世界电信与信息化日大会数据安全与治理分论坛上，中国信息通信研究院安全研究所所长谢玮发表了题为“《数据安全法》引领行业数据安全管理步入新阶段”的主题演讲。

谢玮认为行业数据安全管理的重点是构建行业数据安全工作总体框架。在《数据安全法》和国家数据安全工作协调机制安排下，工业和电信行业承担推进行业数据安全监管、促进数据安全产业发展的两大职责，将按照“5+1”数据安全工作总体框架推进相关工作。

其中，“5”是指紧扣行业监管主线的五大要素，以监管制度和标准规范为基础，以组织体系和工作机制为保障，以技术手段为支撑；“1”则是指的加快落实数据安全产业的发展任务，进一步发挥工业和信息化部产业部门的优势，夯实供给侧产品的技术基础，服务千行百业的数据安全需求。

具体来说，在推进行业数据安全监管方面，将按照“有重点、分领域”的基本思路，以重要数据和核心数据目录为核心开展工作，在建立完善的组织体系基础之上，从构建监管制度、健全工作机制、完善标准规范、强化技术能力四方

面推进相关工作；在促进数据安全产业发展方面，将从加强政策引导、引导技术产品创新、加快产业集聚发展、培育创新生态体系四方面大力促进数据安全产业发展。

http://www.cww.net.cn/article?id=562826

2、张超：实现数据确权与保护，数据密态渐成行业共识

近日，清华大学网络研究院副教授、MIT TR35 China 获得者张超发表文章，阐释了要充分利用创新的技术手段推动数据确权等观点。

张超指出，密态数据的隐私计算技术，解决了数据确权与隐私保护的很多痛点，但是在实践落地中仍然存在挑战，需要进一步融合多种技术甚至与法规相配合，才能更好地推动密态数据的确权、流通与交易等商业应用的实用化落地。

首先，隐私计算单一技术并非所有应用的最佳解决方案，例如在密态数据的登记与检索方面，与区块链技术相结合的隐私计算技术可以更高效地实现密态数据的确权登记、确权记录检索、交易登记、交易记录检索等。

其次，当前的隐私计算面临着效率瓶颈，包括本地计算效率以及网络通信效率等，解决效率问题的技术途径包括针对隐私计算的专用芯片、优化的隐私计算算法等。

第三，隐私计算系统也面临着传统的安全风险，在开放

的网络与系统环境下，其逻辑和数据的完整性可能受到破坏，因而也需要硬件、系统、算法多维度的技术协同，确保隐私计算技术的底座安全性。

最后，技术方案不能完全解决数据确权与合规的问题，需要标准、法规的支持与配合。当某个隐私计算方案失去了其承诺的数据保护能力时，需要通过行业标准、国家标准、法律法规的支持，让业界有规可循，才能实现其商业应用的合规。

http://tech.cnr.cn/techds/20220524/t20220524_525836156.shtml

3、刘洋：联邦学习的效率和安全需要协同发展

联邦学习是目前隐私增强计算与人工智能相结合的新型技术范式，是解决严监管与数据要素价值释放强需求这一矛盾的关键技术思路。清华大学智能产业研究院（AIR）副教授刘洋就联邦学习的安全及效率的平衡问题发表了看法。

从技术角度来说，隐私计算中的安全分为“过程安全”和“结果安全”。

所谓的“过程安全”是在联合计算的过程中，保证传输的内容不被破解和暴露，通常采取的信息保护技术包括同态加密、MPC 等。但即便如此，最终还是需要交换结果信息，比如多方查询等。

因此“结果安全”的核心问题就在于如何保证无法从查询结果中繁衍真实数据或提高繁衍的难度，这其中常用的技术手段包括产品隐私和信息的量化压缩等，从信息的角度来控制。但这类技术会造成模型损失，因此就要在模型损失可控以及安全可控的基础上继续提升效率。

https://mp.weixin.qq.com/s/l0zpyudyMJPldhiGQrG_yw

4、齐向东：补短板、防裸奔，筑牢东数西算的安全防线

“东数西算”工程带来数字经济发展机遇的同时，也面临安全大考。在庞大复杂的场景下，数据的全生命周期都面临巨大的安全风险。奇安信集团董事长齐向东表示，数据安全已经上升到了国家战略层面，是“东数西算”的底板工程，筑牢安全基础，数字经济才能安全腾飞。另一方面，随着“东数西算”的推进，算力需求更大，数据流通节点和数据量更多，东西部协同联动，对数据安全防护水平的要求也会更高。

目前，很多企业机构的数据处在“裸奔”状态，这是数据安全的首要问题。齐向东表示，数据“裸奔”主要有四个特征，即特权账号管理薄弱、权限控制措施不力、API 接口疏于防护、风险感知能力缺失。

对此，齐向东总结出弥补数据安全短板的三大关键措施：

第一是盘清家底。系统梳理业务系统、应用、数据等，

掌握重要的数据存在哪、谁在使用、如何使用，梳理已有安全措施是否应用于重要数据资产的环境，形成数据资产梳理报告。

第二是分级分类。针对不同级别的数据，制定不同的安全策略。

第三是精细防护。围绕重要数据资产进行精细化安全防护，来提高整体防护水平。从对特权账号的全生命周期统一管理、访问的安全管控与审计、数据访问行为的审计、API 接口的防护与态势感知建立的多维度监控来进行全方位的数据安全保障。

https://www.aqniu.com/vendor/83937.html

5、协会观点：企业如何做好数据安全治理

数据安全治理是指在组织数据安全战略的指导下，为确保数据处于有效保护和合法利用的状态，多个部门协作实施的一系列活动的集合。所以说，数据安全治理是与所有人都息息相关的事情。

天津市大数据协会提出做好数据安全治理，有三个要点：

一是“以数据为中心”，就是说我们要围绕数据全生命周期，针对具体业务场景、识别数据安全威胁与风险展开工作。

二是“多元化主体参与”，我们在构建多方治理框架，明确各方职责的同时，将各方数据安全达成共识。

三是“兼顾发展与安全”，坚持以数据开发利用和企业发展促进数据安全，坚持以数据安全保障数据开发利用和产业发展。

因此，数据安全治理的重点事项包括：评估与定位企业大数据能力，经营能力建设；构建应用场景蓝图，推动分析应用有效落地；全面推动数据治理，提升企业数据质量落地；搭建领先数据组织，明确大数据团队工作模式。

https://www.sohu.com/a/550994848_120888965

数据安全事件

1、收集用户数据隐私获利，推特被罚 1.5 亿美元

2022 年 5 月 25 日，据美联社、美国国家公共电台等多家媒体报道，美国司法部和联邦贸易委员会 5 月 25 日宣布了与社交媒体公司推特的和解协议。美国联邦执法官员指控推特在六年内将其收集的用户个人数据用于非法销售广告，推特已同意支付 1.5 亿美元的罚款，以解决其面临的不当使用用户数据的指控。除罚款外，推特还必须接受对其数据隐私计划的审计以及其他限制。

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

2、Clearview AI 因违法收集个人数据遭到英国数据监管机构处罚

近日，英国数据监管机构信息专员办公室（Information Commissioner"s Office，以下简称 ICO） 就人脸识别公司 Clearview AI 违法从 Facebook 等社交媒体和网络搜索中收集人物图像并添加到他们的全球数据库中，对 Clearview AI 处以 750 万英镑的罚款，并要求 Clearview AI 公司从数据库中删除英国居民的数据。根据统计，Clearview AI 已经收集保存了 200 多亿张人脸图像。

https://www.secrss.com/articles/42759

3、印度第二大航司遭勒索软件攻击

2022 年 5 月 26 日消息，印度香料航空公司（SpiceJet）表示，由于内部系统在 5 月 24 日**受“勒索软件攻击”影响，已有多次航班延误，大量乘客滞留机场**。目前香料航空官网只有主页能够正常访问，大部分底层系统和网页均无法加载。

https://www.secrss.com/articles/42834

4、Conti 团伙泄露了一月份俄勒冈州遭袭时被盗的数据

2022 年 5 月 25 日报道，Conti 勒索软件团伙公布了它在 1 月份攻击俄勒冈州林恩县政府服务器时窃取的所有数据。据网络安全专家称，该组织似乎正在自我重组，周三发布了近 1,500 份文件。林县官员表示，他们在意识到自己有备份并确定数据不是特别敏感后，选择不支付赎金。

https://therecord.media/linn-county-oregon-data-leak-conti-ransomware/

5、Verizon 员工信息泄露，被索要 25 万美元

2022 年 5 月 29 日，据 Motherboard 报道，一名黑客获得了 Verizon 的一个数据库，其中包含数百名 Verizon 员工

的全名、电子邮件地址、公司 ID 号和电话号码。

这位匿名黑客表示，他们通过说服一名 Verizon 员工让他们远程访问公司计算机来获取数据。黑客表示他们获得了 Verizon 内部工具的访问权限，该工具显示了员工的信息，并编写了一个脚本来查询和抓取数据库。黑客表示，希望 Verizon 向他们支付 25 万美元（约 168.25 万元人民币）。

https://mp.weixin.qq.com/s/XrBBWFOs8vEXiIAN82L8QQ

6、新型 ERMAC 2.0 Android 恶意软件窃取了 467 个应用程序的帐户和钱包

2022 年 5 月 26 日，ERMAC Android 银行木马已经发布 2.0 版本，目标应用程序增加到 467 个，覆盖更广泛的应用程序以窃取账户证书和加密钱包。该木马的目标是将被盗的登录凭据发送给威胁参与者，然后他们使用它们来控制其他人的银行和加密货币账户并进行金融或其他形式的欺诈。

https://www.bleepingcomputer.com/news/security/new-ermac-20-android-malware-steals-accounts-wallets-from-467-apps/

7、支付巨头 PayPal 曝大漏洞，黑客可直接窃取用户资金

2022 年 5 月 23 日，据外媒报道，一位安全研究人员在支付巨头 PayPal 的汇款服务中发现了一个未修补的漏洞，

可允许攻击者窃取用户账户中的资金。

令人担忧的是，该攻击可能会对与 PayPal 集成以进行结账的在线门户网站造成灾难性后果，从而使恶意行为者能够从用户的 PayPal 账户中扣除任意金额。

https://thehackernews.com/2022/05/paypal-pays-hacker-200000-for.html

8、米高梅 1.42 亿条客户记录遭泄露，影响大约 3000 万人

2022 年 5 月 24 日，据外媒报道，一名黑客通过 NightLion 的 DataViperw 网站窃取了多个数据库。其中一个数据库属于米高梅度假村，包含 1.42 亿客户的个人数据。据 VPNMentor 研究人员称，目前尚不清楚受影响用户的确切数量，但粗略估计表明这次泄漏可能会影响大约 3000 万人。

https://mp.weixin.qq.com/s/9EjBe_BQCe7n5zyuPOBLDg

9、华盛顿大学医学院通知患者数据泄露

2022 年 5 月 24 日，据外媒报道，位于圣路易斯的华盛顿大学医学院通知患者，数据泄露可能会暴露他们的一些个人健康信息。

据获悉，在 3 月 4 日至 3 月 28 日期间，未经授权的人访问了华盛顿大学医学院某些员工的电子邮件帐户。调查

无法确定入侵者是否查看了账户中的任何电子邮件或附件，但卫生系统确实确定这些电子邮件包含患者和研究参与者的信息，包括姓名、出生日期、地址、医疗记录、患者帐号和临床信息。在某些情况下，账户中还包含健康保险信息和社会安全号码。

https://www.beckershospitalreview.com/cybersecurity/washington-university-school-of-medicine-notifies-patients-of-data-breach-2.html?&web_view=true

10、某配置错误的 ES 服务器泄露数百万贷款申请人的信息

2022 年 5 月 24 日，据报道，一个配置错误的 Elasticsearch 服务器泄露了 147 GB 的数据，共 8.7 亿条记录。该服务器于 2021 年 12 月 5 日被检测到，主要包括乌克兰、哈萨克斯坦和俄罗斯小额贷款的申请人的信息，如姓名、住址和护照号码等个人信息，以及薪水、贷款详情和 INN（税号）等财务信息。据估计，约有 1000 万用户受到影响，其中大部分服务器日志和护照号码属于俄罗斯，大多数 INN 属于乌克兰，而该服务器位于荷兰的阿姆斯特丹。

https://www.hackread.com/personal-data-russians-ukrainians-exposed-online/

11、通用汽车透露其遭到撞库攻击导致部分客户的信息泄露

2022 年 5 月 23 日，据报道，美国通用汽车称其在上个月遭到了撞库攻击，泄露了在线平台部分用户的信息。该汽车制造商透露，他们在 2022 年 4 月 11 日至 29 日检测到了恶意登录的活动，发现攻击者已将部分用户的奖励积分兑换为礼品卡。该公司表示，此次违规事件并不是源于通用汽车的系统遭到入侵，而是针对其平台上客户的一波撞库攻击导致的，他们将为所有受影响的用户恢复积分，并建议用户在登陆帐户之前重置密码。

https://www.bleepingcomputer.com/news/security/gm-credential-stuffing-attack-exposed-car-owners-personal-info/