全球数据安全观察

总第 124 期 2023 年第 5 期

(2023.02.06-2023.02.12)

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、国家邮政局强调用户个人信息保护

2 月 6 日，国家邮政局召开局长办公会，会议强调，邮政快递领域用户个人信息保护事关国家安全、公共安全和人民群众生命财产安全，要会同有关部门依法严厉打击泄露、买卖寄递服务用户个人信息等行为，落实好邮政管理部门监管责任，督促寄递企业加强网络安全数据安全和个人信息保护工作。要认真组织抓好规定宣贯落实，健全完善企业信息安全保护责任制，积极推进有效技术手段应用，强化个人信息安全实时监测能力，严密防范和遏制重大安全风险、事件发生。

https://www.spb.gov.cn/gjyzj/c100015/c100016/202302/3bcd44a89fbd4972814cac8d5d40f10b.shtml

2、北京市印发《2023 年市政府工作报告重点任务清单》

1 月 30 日，北京市人民政府印发《2023 年市政府工作报告重点任务清单》，提出着力建设全球数字经济标杆城市，落实北京数字经济促进条例，推动北京数据特区建设，开展数据基础制度先行示范。培育数据要素开放共享新市场，提升国际大数据交易所能级，鼓励各类市场主体进场交易，加

快汇聚行业高价值数据，打造普惠社会数据专区；培育数据评估评价、安全评估等数据要素市场机构，提供数据经纪、登记、评估等全链路服务；在服务数字贸易、数据跨境流通、对接国际数字经济规则方面先行先试。

http://www.beijing.gov.cn/zhengce/zhengcefagui/202301/t20230131_2909785.html

3、广东省全省政务服务和数据管理工作会议召开

2 月 7 日，全省政务服务和数据管理工作会议在广州召开。会议指出 2023 年重点从五个方面发力，推动数字政府建设为广东高质量发展贡献更大力量：一是夯实集约化“大底座”，加强数字政府基础能力建设；二是练好服务与治理“基本功”，抓好数字政府建设的主责主业；三是打出营商环境“组合拳”，有力服务实体经济和制造业；四是下好数据要素“制胜棋”，激活发展新动能；五是打好改革攻坚“主动仗”，促进经济社会全面数字化发展。

http://zfsg.gd.gov.cn/xxfb/ywsd/content/post_4091814.html

4、工信部发布关于侵害用户权益行为的 APP 通报

依据《个人信息保护法》《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，工信部组

织第三方检测机构对群众关注的生活服务类移动互联网应用程序（APP）及第三方软件开发工具包（SDK）进行检查。发现墨迹天气极速版、华为阅读、中国移动云盘、屈臣氏等46款APP（SDK）存在侵害用户权益行为，予以通报。

https://www.miit.gov.cn/jgsj/xgj/fwjd/art/2023/art_c3ab2f3fef674a91892a2da2da452fff.html

5、印度拟在境内设立“数据大使馆”，为数据提供“外交豁免权”

印度财政部长尼尔马拉·西塔拉曼（Nirmala Sitharaman）在她的2023-24年预算演讲中表示，政府将推动在古吉拉特邦国际金融科技城 (GIFT IFSC)建立“数据大使馆”。在古吉拉特邦国际金融科技城(GIFT IFSC)设立的“数据大使馆”将享有与实体大使馆类似的外交豁免权。印度政府还希望通过“数据大使馆”一起解决数据存储和跨境数据流动的问题。

https://www.secrss.com/articles/51684

技术、产品与市场

1、美国 NIST 推出物联网数据保护加密算法

美国国家标准与技术研究院 (NIST) 近日宣布，名为 ASCON 的认证加密和散列算法系列将成为标准算法，用于轻量级密码学应用。该算法中标“轻量级密码学”计划，旨在寻找最佳算法来保护硬件资源有限的小型 IoT（物联网）设备。

小型物联网设备正变得越来越流行和无处不在，用于可穿戴技术、“智能家居”应用等。但是，它们仍然用于存储和处理敏感的个人信息，例如健康数据、财务详细信息等。也就是说，实施数据加密标准对于保护人们的数据至关重要。这些设备内部的薄弱芯片需要一种能够以极低的计算能力提供强大加密的算法。

NIST 仍然推荐高级加密标准（AES）和 SHA-256 用于一般用途，但是这些不适用于资源有限的小型设备。

https://www.bleepingcomputer.com/news/security/us-nist-unveils-winning-encryption-algorithm-for-iot-data-protection/?&web_view=true

2、2023 年网络安全十大发展趋势发布：涉及隐私计算、数据安全

近日，中国计算机学会（CCF）计算机安全专委会中来自国家网络安全主管部门、高校、科研院所、大型央企、民营企业的委员投票评选出 2023 年网络安全十大发展趋势，其中与数据安全相关的部分如下。

趋势一、数据安全治理成为数字经济的基石：数据安全治理不仅是一系列技术应用或产品，更是包括组织构建、规范制定、技术支撑等要素共同完成数据安全建设的方法论。数据、模型算法、算力是数字经济发展的三大核心要素，其中数据是原材料。因此，发展数字经济、加快培育发展数据要素市场，必须把保障数据安全放在突出位置，着力解决数据安全领域的突出问题，有效提升数据安全治理能力。在建立安全可控、弹性包容的数据要素治理制度后，需有效推动数据开发利用与数据安全的一体两翼平衡发展。鉴于此，夯实数据安全治理是促进以数据为关键要素的数字经济健康快速发展的基石。

趋势四、隐私计算技术得到产学研界共同关注：作为平衡数据流通与安全的重要工具，隐私计算成为数字经济的底层基础设施，为各行各业搭建坚实的数据应用基础。近年来，隐私计算产业快速增长，预计 2025 年国内市场规模将达百

亿元，在巨大市场预期下，产学研界将更加关注隐私计算技术的新发展和产品应用的新场景。

趋势五、数据安全产业迎来高速增长：2023 年，《网络数据安全管理条例》有望正式出台。在政策法规和可操作性标准持续优化完善的背景下，在数据合规与企业数据保护的双重驱动下，数据安全产品和服务市场需求更加凸显，以数据为中心的安全投资将获得增长，数据安全产业的增速有望进一步加大。在下游需求及国家政策推动下，各行业对数据安全的投入占比将持续增长，尤其是政务数据管理和央企、国企在相关领域的投入增速将明显加大，有望带动网络安全市场在 2023 年实现一定程度的复苏。

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

3、调查：几乎所有公司都与遭遇过数据泄露的第三方存在业务往来

分析发现，企业平均拥有大约 10 家第三方关系，而间接第四方关系更是高达数百家，一家企业的第四方数量通常高出第三方数量 60 到 90 倍。

几乎每家公司都跟遭受过数据泄露的第三方有业务往来，或者使用其产品，导致自身风险有所增加。

以上结论出自数据科学公司 Cyentia Institute，该公司分

析了网络安全风险管理公司 SecurityScorecard 提供的 23 万家企业的外部安全评估。分析发现，企业平均拥有大约 10 家第三方关系，而间接第四方关系更是高达数百家，一家企业的第四方数量通常高出第三方数量 60 到 90 倍。分析报告指出，几乎所有公司（98%）都至少与一家遭遇过数据泄露的第三方合作伙伴存在业务往来。

https://www.secrss.com/articles/51686

4、调查：错误配置和漏洞成云安全最大风险

Sysdig 的报告指出，软件供应链持续引入的错误配置和漏洞仍是两个最大的云安全风险。

尽管零信任是当务之急，数据却显示，零信任架构的基础——最小访问权限，并未得到妥善执行。报告指出，几乎90%的授权未被使用，给盗取凭证的攻击者留下了很多机会。

以上数据出自对 Sysdig 客户日常运行的 700 多万个容器的分析报告。该报告还考虑了从 GitHub、Docker Hub 和 CNCF 等公共数据源拉取的数据。南北美、澳洲、欧盟、英国和日本的客户数据也是报告分析的对象。

https://www.secrss.com/articles/51639

5、Barracuda：2022 年 75%的组织遭到电子邮件攻击 平均恢复费用为 100 万美元

根据市场调查机构 Barracuda 公布的最新报告，**75% 参与调查的组织在过去 12 个月内都经历过至少 1 次成功入侵的电子邮件攻击。**

研究发现，组织在遭到以电子邮件为载体的安全攻击之后，想要恢复平均要花费 100 万美元。69% 的勒索软件攻击都是从电子邮件开始的。

金融服务组织是黑客最喜欢的攻击目标，该行业 59%受访者表示影响最大的是损失了宝贵的数据; 51% 的受访组织损失了大量金钱。对于医疗保健机构而言，44% 受访组织表示让系统快速启动并再次运行所涉及的恢复成本影响最大。

https://www.anquanke.com/post/id/286251

业界观点

1、陈湉: 近期国内数据相关地方立法动向分析——以深圳、上海为例

2020 年后，建设培育数据要素市场成为数据相关地方立法的主要任务，深圳市、上海市先后出台的数据条例在此方面表现得尤为显著。地方立法的超前探索有益于引导构建数据要素市场体系，回应经济发展需求，促进未来国家层面立法，但需要解决好如何理解和定位数据的财产属性、如何分配数据访问权益/收益权益、如何保护个人信息等关键性问题。欧盟关于数据访问权的立法思路值得我国借鉴。下一步我国的重要工作是做好立法后评估，及时总结经验，保证法律制度始终能够促进数字经济发展。

深圳：自 2020 年 7 月公开征求意见以来，《深圳经济特区数据条例》的立法过程一直广受关注，多项法律制度的创新设计引发了学术界、实务界的热烈讨论。更加特殊的是，该条例的起草编制过程与《数据安全法》《个人信息保护法》的立法过程在时间上存在高度重叠。一方面，如何保持与正在制定的上位法的衔接成为深圳立法工作者必须解决的特有问题；另一方面，在国家数据领域立法工作背景下，条例呈现了与以前数据相关地方性法规不同的鲜明特色。

《上海市数据条例》的立法进程稍晚于《深圳经济特区数据条例》，从条例内容来看，前者在一定程度上受到了后者的影响，也呈现出了与以往数据相关地方立法不同的上海特色。同时，《上海市数据条例》是在《数据安全法》《个人信息保护法》获得通过后，形成的公开征求意见稿，并于2021年11月25日正式通过，因此该条例与两部上位法的衔接更加紧密和顺畅。

深圳市和上海市首开先河，以地方性法规的形式制定数据条例，探索构建数据处理活动的统一规则框架，培育地方数据要素市场，对于我国数据领域立法有着十分重要的积极意义。虽然《深圳经济特区数据条例》和《上海市数据条例》都存在一些遗憾，但其中的创新性制度设计，对其他地方层面立法和国家层面立法都有着重要的借鉴意义。下一步的工作是要做好对这两部条例立法后的评估和修改，特别是对数据财产属性定位、数据相关权益分配、数据交易市场规则等重点方面的规定实施情况要进行深入评估、及时总结、及时调整，使其能够始终对数字经济建设发挥切实、积极的促进作用。

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

2、中国信通院汤立波等：个人信息保护政策标准发展分析

个人信息是大数据时代高价值资产，为信息领域新产品、新服务、新业态发展提供重要支持。个人信息的高价值属性导致信息泄漏事件频繁发生，违规收集个人信息和滥用现象严重，用户权益受到严重侵害。

为规范和引导产业健康发展，欧美和我国都在积极加强个人信息保护政策制定和法律完善，推行符合各自国情的个人信息保护政策法规。

欧盟采取严格立法保护个人信息。欧盟主张全欧盟范围统一、严格的立法。欧盟自 2018 年 5 月起执行《通用数据保护条例》(GDPR)，通过法律强制力对个人信息保护实行严格管理。

美国立法和行业自律相结合推动个人信息保护。美国采取立法与行业自律相结合的方式保护个人信息，主张政府有限干预。立法方面，美国通过联邦立法结合各州分散立法构建基础法律框架。在传统电信行业，以《隐私权法》《信息自由法》《电子通讯隐私法》和《有线通讯隐私权法案》等法律为基础，形成了良好的个人信息保护法律环境。

我国个人信息保护政策法规顶层设计逐步完善。我国个人信息保护立法快速推进，逐步形成较为完善的立法体系。同时，我国政府持续推进政策规章完善，不断强化个人信息

保护监管。

https://mp.weixin.qq.com/s/j_bZn3Y8GYTbZBe55u8ofA

3、加快构建数据基础法律体系

数据是新型生产要素，是推动数字经济深入发展的核心引擎。党的十八大以来，党中央高度重视数据要素的作用发挥，审议通过了《关于构建数据基础制度更好发挥数据要素作用的意见》等文件，为加快构建数据基础法律体系指明了方向。

加快完善数据产权的规范体系。**将数据产权细化为数据所有权、数据占有权、数据支配权、数据使用权、数据收益权**，释放个人数据、企业数据、公共数据的产业效能。

完善数据流通的规则体系。**完善数据要素流通准入规则**，确保数据要素的源头合法，在源头完成信息脱敏，实现数据内容“可界定、可流通、可定价”；**规范场内数据交易流通**，明确主体资格审核、交易规范、市场运营管理等规则，引导数据合法合规交易；**规范场外数据交易流通**，加强场外交易中的数据安全和隐私保护，保障数据提供者的数据权益，促进多种场景下各种数据要素的安全流通；**建立数据要素跨境流通规则**，积极开展数据交互、业务互通、监管互认、服务共享等方面的国际交流合作，搭建离岸数据交易平台，探索

数据“可用不可见”跨境流通环境，探索通过“监管沙箱”等方式提供符合监管要求的数据跨境传输技术和设施。。

推动数据收益合理分配机制的建构。**建立有一定普适性的估值体系**，数据价值链最终产品的价值明确数据的价格形成机制作为数据要素收益分配的基础；**明确相关主体在数据价值创造过程中的贡献**，作为数据收益分配的依据。引入市场机制，动态调整收益分配机制；**完善数据要素市场化配置机制**，发挥政府在数据要素收益分配中的引导调节作用，建立体现效率、促进公平的数据要素收益分配制度。

完善数据安全治理法律制度。数据安全治理应当坚持总体国家安全观，针对不同的数据类型、数据用途、数据敏感程度等，完善分级分类管理办法，维护国家数据安全。同时，还需要构建政府、企业、社会多方协同治理模式，强化分行业监管和跨行业协同监管，压实企业数据安全责任。

http://www.legaldaily.com.cn/index/content/2023-02/08/content_8820184.html

4、着力提升全民数据安全意识和素养

数据安全构成了国家安全的重要组成部分，全民数据安全意识和素养也被认为是推进数字中国高质量建设的基础条件。要着力增强全民数据安全意识和素养，筑牢国家安全

人民防线，树立科学的数据安全世界观和方法论，以新安全格局保障新发展格局，建设更高水平的平安中国。

培养全民数据安全总体意识。包括培养领导者数据安全总体意识。增强企业员工的数据安全总体意识，培养全民数据安全总体意识。

增强数据安全法治意识。积极开展数据安全普法，增强全民数据安全法治意识和素养；普及数据安全理念，抵制数据信息使用不法行为；要强化全民数据安全应用的伦理规范和行为规范，特别是增强新兴职业群体的数据安全法治意识。着力增强数据处理部门业务人员数据安全法治意识，积极营造数据安全全员法治文化机制。

提升全民数据安全基本素养。首先，要具备安全存储个人和组织数据的基本素养。其次，自觉养成避免在公共网络中处理重要数据的习惯。最后，提升全民数据安全问题甄别素养。

开展全民数据安全科普宣传。坚持可持续发展的理念，鼓励各部门、行业和地区制定专门的数据安全意识和素养层面的中长期规划，推进基本业务与全民数据安全意识科普宣传的协同发展。二是鼓励数据安全科普知识进社区、进家庭、进课堂。

https://theory.gmw.cn/2023-02/08/content_36353056.htm

5、ChatGPT 数据安全挑战不可掉以轻心

近期，由于科技公司谷歌、百度跟随微软密集发布类似 ChatGPT 的聊天机器人项目，资本市场卷起一场“ChatGPT”概念旋风。虽然科技巨头陆续入局类 ChatGPT 赛道，但对于其可能带来的风险和挑战也有警惕，先后警告本公司员工不要随意与 ChatGPT 互动。这也引发了公众对于 ChatGPT 是否会带来数据安全风险的担忧。

吴丹君表示，一旦与 ChatGPT 分享机密信息，这些输入的数据可能被用于未来模型的迭代训练，将会导致其所输出的内容可能包含用户提供的个人信息、机密数据或重要数据，造成敏感数据泄漏的风险。

张凌寒表示，除了敏感数据的泄漏风险，ChatGPT 还有以下数据安全风险:

第一，未经用户同意即进行大量的数据抓取，从而存在侵犯个人隐私的风险;

第二，ChatGPT 很难保证在不断的迭代中完全删除其使用的个人信息。

第三，在恶意利用方面，ChatGPT 通过来自社交媒体或者其他文本数据进行模型训练，可能生成虚假信息、诱骗信息等不良信息，破坏网络舆论生态。恶意使用者能够生成大量用户名和密码的组合，用于对在线账户的撞库攻击。

第四， ChatGPT 的自然语言编写能够生成逃避防病毒软件监测的恶意软件，带来网络安全隐患。

为了应对 ChatGPT 可能引发的数据安全问题，张凌寒认为，一方面，需要从法律层面明确有害的类 ChatGPT 产品的应用范围，推进数据分类分级，定义不同类型的数据以确定各类数据的保护级别和保护措施。另一方面，在技术监管中，监控类 ChatGPT 产品的使用情况并定期对其进行安全审计，针对技术应用快速迭代的特征，探索动态评估、修改和废止机制，保障监管的科学化和精细化。

吴丹君认为，开发并使用类 ChatGPT 产品的企业，在数据安全合规方面需要注意三个层面：首先，要保证企业数据来源的安全、可靠，确保已获得处理个人信息的合法性基础；其次，需将算法合规纳入数据安全合规体系，加强技术管理，定期审核、评估、验证算法机制机理。同时，企业还需将伦理道德融入人工智能全生命周期，促进大模型人工智能应用向上向善发展。最后是要加强信息内容管理，建立健全违法和不良信息识别机制和辟谣机制，对输入数据和合成结果进行审核。

https://k.sina.com.cn/article_1684012053_645ffc1501901brqj.html

数据安全事件

1、韩国个人信息保护委员会对 Meta 罚款 660 万韩元

据报道，韩国个人信息保护委员会 2 月 8 日决定，**对违反韩国《个人信息保护法》的 Meta 下达纠正命令、罚款 660 万韩元并要求其采取公开消息等整改措施。**此前，Meta 用户若拒绝授权公司使用本人在其他网站浏览的情况等“轨迹信息”，那就无法继续使用 Facebook 和 Instagram。

此次处置明确表明，**Meta 在用户加入 Facebook 和 Instagram 服务及收集第三方行为信息前，未给予他们拒绝提供第三方行为信息的选择权，这一行为违反了法律。**

https://www.secrss.com/articles/51758

2、因违规查询个人信息 国内知名金融机构消费金融被罚 75 万

2 月 10 日报道，一消费金融公司因因个人信息违规查询而受到处罚。2 月 8 日，央行长沙中心支行发布的罚信息显示，因存在未经同意查询个人信息的违法违规行为，长银五八消费金融被罚款 75 万元。

与此同时，此次罚单实施了“双罚制”，对机构和相关负责人同时进处罚。时任长银五八消费金融风险合规部贷后中

心主任胡少成、风险合规部大数据中心主任许洋分别被处 8 万元罚款，风险合规部总经理唐小杰、风险合规部员工朱虹分别被罚 7 万元。

https://www.wangan.com/p/11v722562ea4a502

3、匿名者组织泄露俄罗斯运营商 128GB 数据，内含 FSB 监控计划

匿名者组织上周发布了 128 GB 的文件，据称这些文件是从俄罗斯互联网服务提供商 Convex 窃取的。庞大的数据宝库由 Anonymous 附属集团 Caxxii 的附属机构租用。被盗文件包含情报部门 FSB 进行的天罗地网监视活动的证据。

据称，这种监视活动被归类为未经授权的窃听、间谍活动和对平民的无证监视，这些都是违反该国法律的。

https://www.secrss.com/articles/51713

4、勒索团伙窃取了加利福尼亚州超过 300 万患者的医疗记录和个人信息

2 月 11 日，据外媒报道，加利福尼亚州的几个医疗组织已向超过 300 万患者发送了安全漏洞通知信，提醒他们在 12 月的勒索软件感染期间，骗子可能窃取了他们大量敏感的健康和个人信息。

从提交给各州和联邦机构的文件来看，勒索者窃取的信息包括：患者姓名、社会安全号码、地址、出生日期、诊断和治疗信息、实验室测试结果、处方数据、放射学报告、健康计划会员号码和电话号码。据正在调查该数据泄露事件的美国卫生与公共服务部称，它影响了 3,300,638 人。

https://www.theregister.com/2023/02/11/ransomware_regal_medical_group/?&web_view=true

5、网络硬件制造商 A10 Networks 确认勒索软件攻击后数据泄露

2 月 10 日，据外媒报道，总部位于加利福尼亚的网络硬件制造商“A10 Networks”已证实，Play 勒索软件团伙短暂获得了对其 IT 基础设施的访问权限并泄露了数据。

根据该公司的调查显示，威胁行为者设法获得了对共享驱动器的访问权限并部署了恶意软件，“泄露”了与人力资源、财务和法律职能相关的数据。

尽管网络被不法分子入侵，该公司表示安全事件并未影响其任何产品或解决方案，也不会影响其客户。

https://www.bleepingcomputer.com/news/security/a10-networks-confirms-data-breach-after-play-ransomware-attack/

6、45 亿国内快递信息泄露，几乎涉及每一个网购过的个人隐私信息

2 月 12 日晚，Telegram 查询机器人：sheg66_bot 爆出国内 45 亿个人信息泄露，最新的数据时间大概来自 2022 年（网友分析具体时间是 2016 年至 2022 年），也就是近几年几乎所有住址信息都暴露了，数据来源主要是各平台快递数据。

据可靠消息，淘宝、抖音等国内知名电商平台疑似泄露超过 45 亿条新的快递地址的数据，包含了真实姓名、电话与住址等信息，并且已出现公开查询渠道。

机器人只支持手机号码查询，查过的普遍反映存在自己的数据，也就是覆盖了国内网购的大部分人员。

根据该机器人管理员提供的 navicat 截图显示，泄露的数据量为 4541420022 条，数据库大小为 435.35GB。

https://mp.weixin.qq.com/s/vGMNawp4dpbNnhBy4tXU3Q

7、Reddit 遭到钓鱼攻击导致内部文件和源代码泄露

媒体 2 月 9 日称，Reddit 遭到网络攻击，业务系统被入侵，内部文件和源代码泄露。攻击发生在上周日晚间，该公司表示，黑客使用了针对 Reddit 员工的诱饵，用一个登陆页面冒充其内网网站，试图窃取员工凭证和双因素认证令牌。在成功窃取一名员工的凭证后，攻击者获得了对一些内部文

档、代码以及一些内部显示面板和业务系统的访问权限。虽然 Reddit 没有公开关于钓鱼攻击的任何细节，但提到了的类似于针对 Riot Games 的攻击。

https://www.bleepingcomputer.com/news/security/hackers-breach-reddit-to-steal-source-code-and-internal-data/

8、黑客 IntelBroker 公开 Weee!约 110 万客户的个人信息

2 月 8 日报道称，亚裔和西班牙裔送餐服务 Weee!约 110 万客户的个人信息泄露。上周一，名为 IntelBroker 的黑客在暗网 Breached 上发帖称，2023 年 2 月，Sayweee 的 1100 万客户的数据库被盗。Weee! 在声明中表示，此次事件影响了在 2021 年 7 月 12 日至 2022 年 7 月 12 日之间下订单的客户，但是付款信息没有泄露。虽然攻击者表示涉及 1100 万客户，但 Have I Been Pwned 称泄露数据仅包括 110 万个唯一的邮件地址，额外的记录很可能是由于同一客户下了多个订单导致的。

hackread.com/weee-grocery-service-hacked/

9、俄罗斯电商公司 e.way 泄露大约 700 万条用户的数据

据媒体 2 月 7 日报道，Cybernews 发现了一个暴露的数据库，包含 1.1TB 数据。研究人员在 1 月 24 日发现了该数

据库，并将其归因于俄罗斯电气工程公司 Elevel 旗下的在线商店 e.way。这个数据库包含 700 万条数据，泄露了两年的客户信息，如姓名、电话号码、电子邮件地址和送货地址等。此外，它包含以 URL 编码的登录数据和密码，这是一种较弱的保护机制，很容易被解码。目前，数据库已经无法访问，但该公司尚未做出回应。

https://cybernews.com/privacy/russian-e-commerce-giant-data-leak/

10、美国 Sharp HealthCare 近 6.3 万患者的支付信息泄露

2 月 6 日报道称，圣地亚哥最大的医疗服务提供商 Sharp HealthCare 通知 62777 名患者，他们的个人信息在运行 sharp.com 的计算机遭到攻击时泄露。报告表明，攻击者在 1 月 12 日只有几个小时的访问权限，且只是影响到在 2021 年 8 月 12 日至 2023 年 1 月 12 日期间使用在线账单支付服务支付账单或发票的患者。Sharp 于 2 月 3 日开始向受影响的患者邮寄通知函，并设立了一个免费呼叫中心以回答问题。

https://www.databreaches.net/sharp-notifies-nearly-63000-patients-of-data-breach-involving-payment-portal/

11、韩国移动运营商 LG Uplus 数据泄露影响约 29 万用户

2 月 10 日消息，据韩联社报道，LG Uplus 上个月的数据泄露事件可能影响约 290000 个用户。

1 月初，该移动运营商曾透露约有 18 万条客户信息泄露，包括姓名、出生日期和电话号码等，但不涉及财务信息。近日，该公司在其网站上表示，发现了另外 11 万条已终止订阅的客户的数据也受到了影响。目前，LG Uplus 正在积极配合当局的调查，事件还在进一步调查当中。

https://www.wangan.com/p/11v724540e32b494