全球数据安全观察

总第 128 期 2023 年第 9 期

(2023.03.06-2023.03.12)

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、《党和国家机构改革方案》通过，将成立国家数据局

近日，党的二十届二中全会通过了《党和国家机构改革方案》，深化国务院机构改革是其中的一项重要任务。任务指出要组建国家数据局，负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等，由国家发展和改革委员会管理。

http://www.gov.cn/xinwen/2023-03/11/content_5745977.htm

2、证监会发布《证券期货业网络和信息安全管理办法》

2 月 27 日，《证券期货业网络和信息安全管理办法》公布，对网络和信息安全管理提出规范要求，主要内容包括：网络和信息安全运行、投资者个人信息保护、网络和信息安全应急处置、关键信息基础设施安全保护、网络和信息安全促进与发展、监督管理和法律责任等。

http://www.csrc.gov.cn/csrc/c101953/c7202800/content.shtml

3、《云南省数字政府建设总体方案》发布

3 月 2 日，云南省人民政府印发《云南省数字政府建设

总体方案》，从总体要求、总体架构、主要任务和重点工程、等方面明确了至 2025 年底的数字政府建设方案。

https://www.yn.gov.cn/zwgk/zfxxgkpt/fdzdgknr/zcwj/zdgkwjyzf/202303/t20230307_255866.html

4、团体标准《信息通信及互联网行业企业合规管理体系 指南》正式发布

3 月 2 日，中国互联网协会发布团体标准 T/ISC 0023-2023《信息通信及互联网行业企业合规管理体系 指南》，规定了信息通信及互联网企业建立、实施、评估、维护及改进合规管理体系的总体指南。

https://www.isc.org.cn/article/15761933709471744.html

技术、产品与市场

1、IDC：国家数据局组建推动数据要素流通，大数据及数据治理市场进一步发展

国家数据局的建设，解决了国家自上而下的统一组织，改变现有的运行方式、运行结构及建设思维。数字基础设施和数据资源体系是数字中国建设的“两大基础”，需要对数据资源规模和质量进行大幅提升。大数据平台作为数字基础设施的关键能力，支撑政务服务、东西部算力的高效协同，一直保持较高的年复合增长率。同时，通过数据治理加快数据的汇聚融合，形成的高质量、高价值数据是数据资源体系的核心。国家数据局的成立带来很多市场机会:

(1) 数据要素管理制度更加完善;

(2) 培育数据要素交易市场;

(3) 促进建设大数据平台，提升数据量及数据质量;

(4) 持续推动数据资源平台的投资建设;

(5) 提升区块链隐私计算解决数据流通安全问题;

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

2、ITDR：增强企业数字身份保护能力的新利器

随着数字身份数量激增，如何加强身份保护和管理成为

许多安全负责人关注的焦点。

在 IAM（统一身份管理）、PAM（特权访问管理）以及 IGA（统一身份管理和治理）等现有的身份保护解决方案中，主要侧重于确保用户访问行为的安全与可控，授权和验证是这类的技术方案关注的重点，但它们往往难以帮助用户及时掌握身份攻击活动中的其他一些关键因素：账号是否滥用、风险暴露面以及权限提升等异常行为。

企业需要将主动端点防御、实时事件响应、零信任基础设施和域名保护等防护措施结合起来，构建更强大的新型身份管理解决方案。Gartner 认为身份威胁检测和响应（ITDR）可以帮助企业填补在身份威胁监测与响应领域的防护空白，不仅可以在企业现有的身份管理模式基础上实现能力增强，还可以与 EDR、NDR 以及 XDR 等威胁监测解决方案互为补充。

https://www.secrss.com/articles/52578

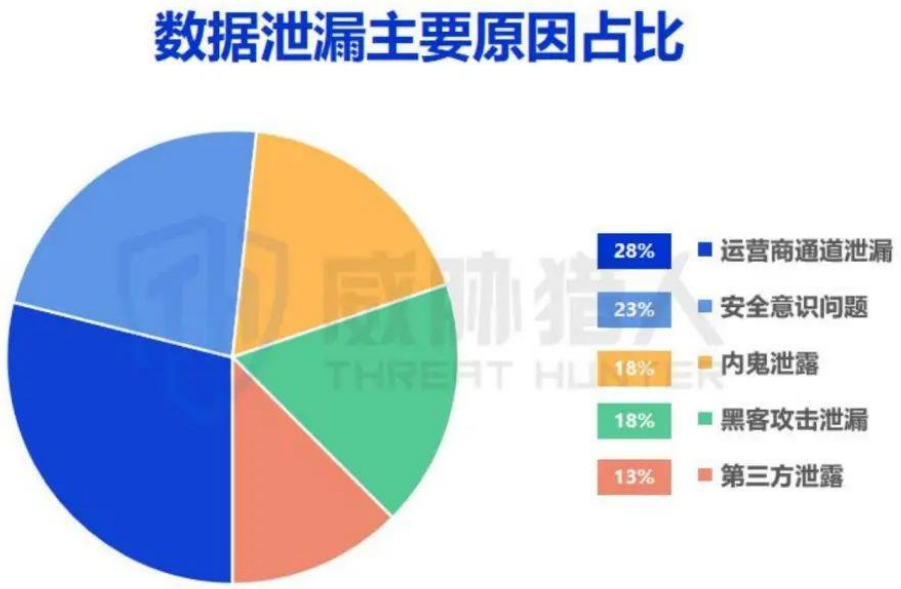
3、《2022 年数据资产泄露分析报告》发布

威胁猎人于近日正式发布《2022 年数据资产泄露分析报告》，较为详尽地展现了 2022 年数据泄露风险的整体概况，以及对其监测到的 2022 年地下黑市数据交易分析成果：

- 2022 年累计捕获数据泄露事件超 3200 起，较 2021

年上升近一倍。

- 数据泄露渠道来源广泛，匿名社交软件占比超 75%。
- 2022 年数据泄露行业分布中，金融、物流、电商行业占据前三。
- 2022 年数据泄露的主要原因中，运营商通道泄露占比第一。



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

4、上海探路数据交易资产化，国内首个数据交易链问世

3 月 3 日，由大数据流通与交易技术国家工程实验室与上海数据交易所正式启动国内首个数据交易链的建设工作，这也是国内数据流通交易领域的新一代基础设施建设项目。

上海数据交易所数据交易系统建立了登记、挂牌、交易、交付、清结算和凭证发放六大业务环节，通过建立数据交易链，利用区块链存证和智能合约等技术使这些业务环节更加安全、高效和透明。区块链技术将数据交易系统的业务环节上链，大大提高数据交易的效率、安全性和透明度，使得交易参与主体互信互认，为各方从登记、确权到交付的交易全过程提供安全保障，体现交易所监管客观公正。

https://mp.weixin.qq.com/s/KuayR-_zkasZN_pUW7Pg9Q

5、依法严惩侵犯公民个人信息犯罪，2022 年检察机关起诉 9300 余人

近年来，检察机关以习近平法治思想为指引，深入贯彻落实党中央决策部署，积极推动个人信息保护法、数据安全法等法律法规统一正确实施，不断强化公民个人信息保护力度，依法保障人民群众合法权益，维护社会安全稳定。2022 年共起诉侵犯公民个人信息犯罪 9300 余人。

侵犯公民个人信息犯罪基本态势:

（1）案件数量保持在高位。2020 年，全国检察机关起诉侵犯公民个人信息犯罪 6000 余人，2021 年起诉人数攀升至 9800 余人，2022 年起诉 9300 余人，近三成被告人被判处三年以上有期徒刑。

（2）自然人犯罪占多数，共同犯罪比例较高。侵犯公民个人信息犯罪绝大多数为自然人犯罪，其中，无业人员占40%；共同犯罪人数占比达 65.7%，犯罪分子多具有较为明确的分工，趋于团伙化。

（3）犯罪手段多样化、网络化、产业化。侵犯公民个人信息犯罪中，有的是行业“内鬼”泄露、倒卖个人信息，有的是通过黑客技术入侵后窃取，有的是通过网络购买、出售，犯罪手段、方法趋于多样化。

（4）被侵害的个人信息类型多、范围广，且与下游犯罪密切相关。被侵害的公民个人信息类型多样，基本覆盖群众生活方方面面，如电话号码、房产信息、车辆信息、信贷信息等，甚至还有绑定电话号码的社交账号，导致被害人变成“透明人”。

暴露出的主要问题：

（1）行业“内鬼”泄露个人信息问题严重。

（2）APP 非法收集个人信息问题突出。

（3）网络聊天工具沦为个人信息交易渠道。

（4）个人自我保护意识还需进一步提高。

https://www.spp.gov.cn/xwfbh/wsfbh/202303/t20230302_605284.shtml

业界观点

1、王源：国家数据局对中国数据治理格局的影响

根据十四届全国人大一次会议表决通过《关于国务院机构改革方案的决定》，中国组建国家数据局，由国家发展和改革委员会管理。以下从机构定位、职能职责、待探索事项三个方面进行梳理和分析。

（1）国家数据局的机构定位

国家数据局是由发改委管理的国家局，为副部级单位。中央网信委和发改委（创新和高技术发展司）承担的数字和数据发展智能划入国家数据局，但不涉及网信办的职能改变，国家数据局成立后，“把数据资源整合共享和开发利用方面的有关职责相对集中”，**国家层面数据治理中的“安全”问题归网信办，“发展”归发改委（国家数据局）**。

（2）国家数据局的职能职责

根据《关于国务院机构改革方案的说明》，国家数据局负责**协调推进数据基础制度建设，统筹推进数字中国、数字经济、数字社会规划和建设等**。

上述职能具体体现在《数字中国建设整体布局规划》（2023 年 2 月 27 日）和《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》（2022 年 12 月 2 日）

（“《数据二十条》”）中，更具体一些体现在《数据安全法》（2021 年 9 月 1 日）中，具体制度性规则（而非概念性或者原则性的方向规定）主要体现在《数据安全法》第二章（数据安全与发展）和第五章（政务数据安全与开放），包括如下三项：数据交易管理制度、数据分类分级保护制度、政务数据和公共数据开放利用制度。

（3）国家数据局的待探索事项

和地方政府大数据管理部门关系：在本次国务院机构改革设立发改委管理的国家数据局之前，地方政府实际上已经设立大数据管理部门，对数据利用进行管理。这些大数据管理部门名称不一，隶属机构和级别从正处到正厅均有，还有一半以上的省没有大数据管理部门。**国家数据局从中央层面和地方政府对数据的管理职责有待厘清**。

跨境数据流通和数据出境安全评估、网络安全审查的平衡：网信部门（中央网信委和网信办）对网络安全、信息内容安全、个人信息保护和算法等监管职责不会改变，包括《网络安全审查办法》《数据出境安全评估办法》确立的网络安全审查制度和数据出境安全评估制度，实际上《数据安全法》中的出口管制等监管职责也不会发生改变。但是数据出境制度和数据分类分级制度会面临更多的跨部门协调问题。数据流通是在国内和国际两个市场循环的，《数据二十条》的第十

一条任务包括构建数据安全合规有序跨境流通机制，开展数据交互、业务互通、监管互认、服务共享等方面国际交流合作，推进跨境数字贸易基础设施建设。多一些安全考量，网信部门负责的出境安全评估和网络安全审查就会严格一些；多一些发展考量，国家数据局负责的跨境流通环境就会宽松一些，尤其是持有100万个人信息的平台海外上市的网络安全审查。

数据分类分级中和国家安全部门的协调：《数据安全法》不仅规定了各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，还规定了国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。因此对数据进行分类分级，尤其是核心数据和重要数据的分类分级不仅涉及数据利用，更涉及数据安全。**其中对重要数据的界定是关键，构成重要数据的标准严格，数据利用空间就大一些；构成重要数据标准宽松（把什么都归为重要数据），数据利用空间就小一些**。数据价值和数据数量成正比，和匿名化或者脱敏程度成反比。重要数据的界定还涉及到平台劳动成果和商业秘密，也是在分类分级需要考量的因素。因此，《数据安全法》中的国家数据安全工作协调机制究竟由谁牵头对于重要数据目录的制定就有重要影响，安全部门、网信部门、还是

国家数据局统筹？

https://www.secrss.com/articles/52653

2、王鹏：国家数据局解读——数字中国建设迎来重大发展机遇

成立国家数据局可以更好发挥政府对数字要素市场的监督管理作用，责任更加具体、清晰，对实现“数字中国”目标具有重要意义与深远影响：第一，有助于建立分工明确、协同推进的多层次数据要素市场建设工作机制，避免各部门、各地方重复建设。第二，利于健全数据要素权益保护制度、建立合规高效的数据要素流通和交易制度、完善数据全流程合规和监管规则体系，建设规范的数据交易市场。第三，统筹规划发挥制度优势，集中力量办大事，对于加快形成数据要素市场体系、促进数字经济高质量发展具有重要意义。

国家数据局的成立只是我们实现“数字中国”的第一步，要想快速实现部门职能、稳定市场情绪等还需要做到以下几个方面：

第一，新的政府部门成立需要将人力、财力等资源补给到位，财政拨款、财政预算需要相关部门精准核算，有针对性的进行专业人才招聘，帮助国家数据局平稳落地。

第二，建立部门规章制度体系，明确部门内部分工，对

内制定内部约束规章制度，对外公布办事流程图，让每一个业务都有章可循。

第三，在工作移交环节中，与网信办、工信部等部门要相互协调，做到工作无缝衔接，避免出现短暂的“三不管”真空期。

在实现“数字中国”的道路上充满了挑战与困难，梳理各地在数据相关实践中存在的难题，对国家数据局有以下期望:

第一、国家数据局未来可以逐渐打通数据从中央部委到最基层的梗堵，要制定国家级法规，采取措施，要求各同级部门之间的数据链接起来，形成数据合法、合规、安全、有序、自由的流动的数据通道。

第二、国家数据局可以保障一些区县的合理的数据要素价值拥有权，还存在一些地市不允许区县有数据持有权的情况。

第三、国家数据局对数据的全流程进行监管、尽快明确国家级数据交易所，避免当前的各地数据交易所严重内卷，重复建设，上架产品雷同等情况。

第四、国家数据局在国家发改委的强势部委的主管下，在国家资金投入、政策支持方面，可以采用数据要素专项债、低息贷款之类的，支持城市和与数据相关的企业。

https://column.chinadaily.com.cn/a/202303/09/WS640987b9a31

02ada8b232b7a.html

3、朱克力：国家数据局破解“九龙治水” 强化统筹发力

国家数据局的组建，国研新经济研究院创始院长朱克力认为其标志性意义体现在三方面。

首先，**彰显我国对数据治理和利用的重视**，为数据要素基础制度建设提供了组织保障，有利于数字中国、数字经济、数字社会的规划和建设的统筹协调，避免“九龙治水”。

其次，**体现我国对数字化转型的战略决心**，为推动数据资源整合共享和开发利用、促进信息资源跨行业跨部门互联互通、提高数据资源价值创造能力提供了政策引导。

最后，**助力国家治理体系和治理能力现代化**，为协调推动公共服务和社会治理信息化、促进智慧城市建设以及保障国家重要信息资源开发利用与共享提供了机构支撑，更好地构建数据基础制度体系，发挥数据要素的作用，提高数据要素治理效能。

接下来，包括数字政府、数字经济、数字社会规划和建设，都将迎来更大的发展契机。

一是**科技创新驱动的发展契机**。随着新一轮科技革命和产业变革的加速推进，数字技术不断创新突破，为各领域数字化转型提供了强大的技术支撑和动力。

二是**市场需求拉动的发展契机**。人民群众对美好生活的向往不断增强，对公共服务、消费升级、社会治理等方面的需求不断增加，为各领域数字化转型提供了广阔的市场空间和需求导向。

三是**制度保障促进的发展契机**。国家在数据资源管理、数据安全保护、数据开放利用等方面制定完善相关法律法规和标准规范，为各领域数字化转型提供了有力的制度保障和指导。

当然，发展数字经济、建设数字中国是一个系统工程，涉及多个方面的协调和配合。具体到工作执行中，政府、企业等主体仍然面临许多困难和挑战，包括数字基础设施建设不足、数据资源管理和开放共享水平亟待提高、数字技术创新能力不强、数字化转型推进有待加快，等等。

针对这些困难和挑战，政府、企业等主体不妨采取一系列应对措施，包括**加大数字基础设施建设投入，提高网络质量和速度，扩大网络覆盖范围，促进城乡区域均衡发展；建立健全数据治理体系和标准规范，加强数据安全保护和监管，推动数据开放共享和流通利用；加快推进数字化转型升级，深化数字技术与实体经济融合，拓展数字化应用场景和服务模式，加强数字化人才培养和引进等**。

http://m.eeo.com.cn/2023/0310/581184.shtml

4、张英：建议上海设立数据国际合作试验区，对标数字经济国际规则

在2023年全国两会上，全国政协委员、上海市经信委副主任、农工党上海市委副主委张英提交了一份《关于释放数据要素潜力更好赋能高水平对外开放的提案》。

她认为，目前我国在推动建立与国际经贸往来相适应的数据流动机制方面，主要有三方面不足：一是对标高标准国际规则相对滞后；二是数据国际合作与流动的试点路径不够清晰；三是数据跨境流动缺少场景思维。

针对上述问题，张英在提案中给出三点建议：

一是对标DEPA等数字经济规则，率先**在上海自贸区临港新片区等地区，开展规则的综合集成和压力测试，设立高标准规则集成的数据国际合作试验区**。积极参与数据流动、数据安全、认证评估、数字货币等国际规则和数字技术标准制定。

二是**完善场景牵引下的数据流动机制和规则**，聚焦全球经贸合作、高端产业开放、国际创新协同等经济数字化转型关键领域场景，完善操作指引，更好服务中国式现代化和韧性供应链体系构建。

三是**创设面向国际数据合作的关键基础设施**，增强国际间连接能力与算力协同，加强区块链、隐私计算等技术应用，

探索“数据可用不出境”等新机制、新模式。依托上海数据交易所等国家级数据交易所，设立数据交易国际板。

https://www.sohu.com/a/650183774_260616

5、谢京：建议支持海南探索国际数据中心试点

在今年全国两会上，住琼全国政协委员、海南省副省长、农工党海南省委会主委、省科技厅厅长谢京向大会提交提案，建议支持海南探索国际数据中心试点。

提案建议，**支持海南探索国际数据中心试点**。按照“特定区域、特定对象、特殊授权、特殊监管”的试点思路，发展“两头在外”“来料加工”的国际数据加工、交换中心等业务，打造“境内关外”数据实验区。推进以“游戏出海”数据服务等为试点，**探索设立国际数据交易中心，搭建数字产品国际交易平台**。推动数据跨境流动在海南自贸港先行先试，形成国际数据产业新优势，打造具有国际影响力的国际数据跨境流动枢纽。

提案还建议，**支持海南开展全业务国际通信出入口局试点**。随着海南—香港光缆建成投入使用，以及还在积极筹建其他以海南为起点的海上丝绸之路方向海缆，海南亟须建设我国第四个全业务国际通信业务出入口局，通过全业务国际通信出入口局与国际网络直接连接，**支撑海南自贸港的发展**

和探索建设数字自由港，将海南发展成为亚太区域先进、通达全球的国际海缆枢纽，服务于“一带一路”沿线中资“走出去”企业的信息化需求，以及海上丝绸之路沿线国家的国际数据通信发展需求。

https://zsyz.contacthainan.gov.cn/zchz/xgzq/202303/t20230307_3422186.html

数据安全事件

1、因违规收集用户信息被罚 1000 亿韩元，消息称谷歌、Meta 不服裁决提起诉讼

据韩联社报道，3 月 6 日，有行业消息人士透露，谷歌和 Meta 已对韩国数据保护监管机构的罚款裁决提起诉讼。

去年 9 月，韩国个人信息保护委员会（PIPC）认为谷歌和 Meta 在未征得用户同意的情况下收集个人信息，并将其用于个性化在线广告和其他目的，因此对这两家公司共计处以总计 1000 亿韩元（IT 之家备注：当前约 5.31 亿元人民币）的罚款。

其中，PIPC 对 Google 处以 692 亿韩元（约 3.47 亿元人民币）罚款，对 Meta 处以 308 亿韩元（约 1.55 亿元人民币）的罚款。谷歌和 Meta 当时对这一决定表示反对，称公司高度重视法律合规以及对用户控制和透明度的承诺。

https://www.ithome.com/0/677/715.htm

2、长沙首张罚单！违反《数据安全法》罚款 5 万元！

近日，长沙市公安局岳麓分局网络安全保卫大队查处了长沙市首起违反《中华人民共和国数据安全法》的行政案件，对涉案公司依法处以行政警告，并处罚款 5 万元。

经查，该涉案公司相关服务器存在未授权访问漏洞，用户隐私数据存在泄露风险。经过进一步核实，该公司未制定数据安全管理制度、未开展等级保护备案工作，严重违反了《中华人民共和国数据安全法》第二十七条、第二十九条规定。

https://mp.weixin.qq.com/s/L0kQgLPD_Zz0zCgsVqBOlA

3、勒索软件团伙泄露从明尼阿波利斯学校盗出的数据视频

3 月 8 日，据外媒报道，美杜莎（Medusa）勒索软件团伙要求明尼阿波利斯公立学校 (MPS) 学区支付 100 万美元的赎金，以删除据称在勒索软件攻击中窃取的数据。

这种勒索企图之所以引人注目，是因为威胁行为者制作了一段视频，该视频显示了据称从明尼阿波利斯公立学校区窃取的所有数据。该教育组织表示，MPS 不打算向威胁行为者支付赎金，而是选择使用内部备份来恢复勒索软件行为者

加密的数据。

https://www.bleepingcomputer.com/news/security/ransomware-gang-posts-video-of-data-stolen-from-minneapolis-schools/

4、弗吉尼亚州一城市声称遭到 BianLian 勒索软件攻击

3 月 9 日，据外媒报道，弗吉尼亚州韦恩斯伯勒市的官方网络门户网站声称受到 BianLian 勒索软件操作的破坏。

BianLian 在其数据泄露网站上发布的一篇帖子中指出，它从韦恩斯伯勒的网络中窃取了 350GB 的数据，包括文件服务器数据和公共关系文件，以及警察局内部文件服务器的数据，其中包括刑事调查、内部文件、工作人员的个人资料、报告和手册等等。

https://www.scmagazine.com/brief/ransomware/virginia-city-claimed-to-be-attacked-by-bianlian-ransomware?&web_view=true

5、美国两院议员及家人身份数据全泄露，已在暗网兜售

3 月 10 日消息，据美国众议院领导人向全体成员发出的通报函和参议院最高安全官员公布的备忘录，国会议员及华盛顿特区居民使用的在线健康保险市场 D.C. Health Link

遭到黑客攻击，导致数千名立法者、其配偶、家属和雇员的个人身份信息面临泄露风险。

作为在线健康保险市场，D.C. Health Link 为大约 1.1 万名国会议员及其工作人员提供服务，总用户数量近 10 万人。由于此次违规行为，联邦调查员已经能够在暗网上买到关于国会议员及其家人的个人信息，此次事件被称为“严重的安全违规”。

据调查，泄露的数据包括：全名、注册日期、关系（本人、配偶、孩子）和电子邮件地址，但并不涉及其他个人身份信息。

https://www.secrss.com/articles/52652

6、美国众议院议员和工作人员数据被盗，FBI 介入调查

3 月 9 日，Bleeping Computer 网站披露，美国联邦调查局（FBI）正在调查一起影响美国众议院议员和工作人员的数据泄露事件。据悉，被盗的敏感个人数据信息来自 DC Health Link 的服务器。（注：DC Health Link 是管理美国众议院议员、其工作人员及其家属的医疗保健计划的组织。）

该事件可能暴露了数千名参保者的个人身份信息（PII）。作为有资格通过华盛顿特区健康链接获得健康保险的会员或雇员，用户的数据可能已经被泄露。

目前，尚不清楚泄密的规模和范围，但黑客论坛上正在出售一份带有数据库标题的被盗数据样本，其中包含大约 170000 名受影响个人的信息，包括他们的姓名、出生日期、地址、电子邮件地址、电话号码、社会保险号码等。

https://www.freebuf.com/news/359844.html

7、黑客论坛上出售宏碁 160 GB 敏感数据

3 月 7 日报道，中国台湾电脑巨头宏碁证实，在黑客成功入侵一台存有维修技术人员私人文件的服务器后，公司遭遇了数据泄露。

2023 年 2 月中旬，一名未知攻击者陆续在黑客论坛上出售声称是从宏碁窃取来的 160GB 数据。该数据泄露事件发生后，该公司发言人表示公司的一个文档服务器出现了漏洞，但截至目前，这一安全事件并未影响客户数据。

从威胁攻击者的说法来看，被盗数据主要包含宏碁公司的技术手册、软件工具、后台基础设施细节、手机、平板电脑和笔记本电脑的产品型号文档、BIOS 图像、ROM 文件、ISO 文件和替换数字产品密钥（RDPK）等。

https://www.bleepingcomputer.com/news/security/acer-confirms-breach-after-160gb-of-data-for-sale-on-hacking-forum/

8、BlackCat 泄露宾夕法尼亚医院患者的数据及诊断照片

3 月 6 日，据外媒报道，勒索软件团伙 BlackCat 泄露了从宾夕法尼亚州一家医疗保健集团（LVHN）窃取的数据，包括乳腺癌患者的诊断截图以及图像。

该集团在宾夕法尼亚州东部经营着 13 家医院以及众多诊所。据调查，2 月 6 日，LVHN 的 IT 团队就在其 IT 系统中检测到未经授权的活动，泄露事件发生后，BlackCat 要求支付赎金，但 LVHN 拒绝支付。

https://www.inforisktoday.com/blackcat-leaking-patient-data-photos-stolen-in-attack-a-21381

9、中资著名手机品牌疑似被黑，11GB 内部敏感数据泄露

3 月 7 日消息，一家数据泄露市场的用户 LeakBase 宣称，已成功通过故障和错误获得了中资背景的美国摩托罗拉公司 JIRA 系统的备份控制面板访问权限。

据用户 LeakBase 透露，外泄的数据包括管理面板（即管理后台）数据，以 HTML 格式导出并带有截屏内容。该用户还提到，数据包含多种文件格式，总大小约为 11 GB。

通过对泄露网站上共享的数据进行初步分析，分析师发现信息内容真实有效。外媒 Cyber Express 已经就此事向摩托罗拉发出置评请求。

https://www.secrss.com/articles/52544

10、西班牙格拉纳达议会近 3GB 的信息在黑客论坛被出售

据外媒 3 月 7 日报道，西班牙格拉纳达议会近 3GB 的信息在黑客论坛被出售。格拉纳达议会是一个公共实体，为公民提供直接服务，并为西班牙格拉纳达省市议会提供技术、经济和技术支持等。据报道，一个名为“GhostSec”的黑客组织将格拉纳达议会数据库列为 dipgra.es 出售，声称拥有近 3 GB 的信息，包括用户名、密码、电子邮件地址等。根据 GhostSec 的说法，这些数据于 12 月下旬获取，目前数据已被售出。

http://www.anquan419.com/knews/24/4574.html

11、知名网络安全公司 Acronis 疑遭黑客攻击

3 月 10 日报道，一位匿名黑客宣称成功入侵了瑞士网络安全公司 Acronis，并在暗网论坛上泄露了从该公司窃取的数据。

Acronis 是知名的老牌数据安全和网络安全公司，在全球拥有超过 2000 名员工，年收入超过 1.2 亿美元。在其官网上，Acronis 宣称能够“通过第一时间阻止攻击发生，主动保护数据、系统和应用程序。”

据称，泄露的数据包括证书文件、命令日志、系统配置、系统信息日志、文件系统档案、Maria.db 数据库的 Python 脚本、备份配置内容以及备份操作的屏幕截图。

https://www.secrss.com/articles/52649

12、宝马暴露了意大利客户的数据

3 月 10 日报道，Cybernews 研究人员发现，BMW 暴露了由 BMW Italy 所依赖的框架生成的敏感文件，可能会泄露其商业机密和客户数据。

2 月，Cybernews 研究人员偶然发现了 BMW Italy 官方网站上托管的未受保护环境(.env) 和.git 配置文件。环境文件(.env) 存储在本地，包括有关生产和开发环境的数据。如果恶意黑客发现了这个漏洞，他们可以利用它来访问客户数据、窃取公司的源代码，并寻找其他漏洞进行利用。

“这一发现表明，即使是知名和值得信赖的品牌也可能具有严重不安全的配置，从而允许攻击者破坏他们的系统以窃取客户信息或通过网络横向移动。”研究人员表示。

https://securityaffairs.com/143297/data-breach/bmw-exposes-clients-italy.html?web_view=true

13、美国电信巨头 AT&T 在供应商遭受黑客攻击后致 900 万客户数据泄露

3 月 9 日，据外媒报道，美国电信巨头 AT&T 通知了大约 900 万客户，他们的一些信息在 1 月份一家营销供应商遭到黑客攻击后泄露。

AT&T 表示:“一些无线账户的客户专有网络信息被泄露，例如账户的线路数量或无线费率计划。但这些信息不包含信用卡信息、社会安全号码、账户密码或其他敏感的个人信息。我们正在通知受影响的客户。”

虽然数据泄露通知没有透露受影响客户的数量，但 AT&T 声称大约有 900 万个无线账户的客户专有网络信息被访问过。暴露的客户专有网络信息数据包括：客户名字、无线帐号、无线电话号码和电子邮件地址。

https://www.bleepingcomputer.com/news/security/atandt-alerts-9-million-customers-of-data-breach-after-vendor-hack/?&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： 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/