全球数据安全观察

总第 91 期 2022 年第 19 期

（2022.05.30-2022.06.05）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、中共中央办公厅 国务院办公厅《关于推进实施国家文化数字化战略的意见》印发

近日，中共中央办公厅、国务院办公厅印发了《关于推进实施国家文化数字化战略的意见》（以下简称《意见》），并发出通知，要求各地区各部门结合实际认真贯彻落实。

《意见》明确，到“十四五”时期末，基本建成文化数字化基础设施和服务平台，形成线上线下融合互动、立体覆盖的文化服务供给体系。到2035年，建成物理分布、逻辑关联、快速链接、高效搜索、全面共享、重点集成的国家文化大数据体系，中华文化全景呈现，中华文化数字化成果全民共享。

《意见》提出了八项重点任务：一、统筹利用文化领域已建或在建数字化工程和数据库所形成的成果，关联形成中华文化数据库。二、夯实文化数字化基础设施，依托现有有线电视网络设施、光电5G网络和互联互通平台，形成国家文化专网。三、鼓励多元主体依托国家文化专网，共同搭建文化数据服务平台。四、鼓励和支持各类文化机构介入国家文化专网，利用文化数据服务平台，探索数字化转型升级的有效路径。五、发展数字化文化消费新场景，大力发展线上

线下一体化、在线在场相结合的数字化文化新体验。六、统筹推进国家文化大数据体系、全国智慧图书馆体系和公共文化云建设，增强公共文化数字内容的供给能力，提升公共文化服务数字化水平。七、加快文化产业数字化布局，在文化数据采集、加工、交易、分发、呈现等领域，培育一批新型文化企业，引领文化产业数字化建设方向。八、构建文化数字化治理体系，完善文化市场综合执法体制，强化文化数据要素市场交易监管。

https://mp.weixin.qq.com/s/X6EM6ELZYIQCjiK7quTxKg

2、辽宁将实行数据安全责任制和分类分级保护制度

5 月 31 日，《辽宁省大数据发展条例》（以下简称“条例”）经省十三届人大常委会第三十四次会议表决通过，将于 2022 年 8 月 1 日正式施行。

条例共九章、五十四条。为解决辽宁省数据要素市场发育不充分问题，补齐要素市场短板，完备要素市场化配置机制，条例设置“数据要素市场”专章，明确了市场主体在数据采集、加工、使用、交易等基本权益方面的保障性规定，给企业吃下“定心丸”；同时，对数据交易和竞争行为以“负面清单”方式划定禁区，就交易市场配套制度建设予以规定，并对违法交易、侵害其他市场主体合法权益等行为增设了处

罚条款。

条例设置“数据安全”专章，**规定实行数据安全责任制和分类分级保护制度，明确责任确定原则，搭建数据安全管理体制**，并就全社会各主体建立落实数据安全保护制度、强化数据存储管理和应急处置等予以明确。

https://mp.weixin.qq.com/s/IwmNsHutH1tx68fyX4QC8w

3、《江苏省数字经济促进条例》将于今年 8 月施行，筑牢数字安全，加快打造数字经济创新发展新高地

5 月 31 日，省十三届人大常委会第三十次会议审议通过《江苏省数字经济促进条例》，将于 8 月 1 日施行。此条例为做强做优做大数字经济作为转型发展的关键增量提供法律保障，并以此促进数字经济创新高质量发展。

该条例结合了江苏省的实际情况，规定要建立数字经济关键核心技术攻关新型体制机制，支持企业、科研机构、高校聚焦重点领域，提高基础研发能力，突破关键核心技术；同时，引导企业与科研机构、高校开展数字经济产学研合作，共建创新平台，推动获取重大原创科技成果和自主知识产权。该条例明确了江苏省要实施全省数字基础设施发展规划，支持完善通信网络、算力等信息基础设施，建设物联网、车联网等融合基础设施，布局创新基础设施，推动传统基础设施

数字化升级，构建数字基础设施体系。

https://mp.weixin.qq.com/s/nY1lZV0sySc42nk1AjDuYA

4、沈阳推行首席数据官制度，全力打造“东北数字第一城”

6 月 1 日，沈阳市大数据管理局副局长洪伟在沈阳市政府新闻办召开的发布会上表示，为完整准确全面落实新发展理念，深化数据要素市场化配置，全力打造“东北数字第一城”，建立跨部门、跨层级、跨领域、跨业务的数字政府协同管理体系，沈阳市制发了《沈阳市推行首席数据官制度工作方案》。推行首席数据官制度是沈阳加快政府数字化转型工作的一项创新举措，主要目标就是要在市区两级政府内部建立起一支“懂业务、懂技术、懂管理”的复合型干部队伍，通过不断提升沈阳首席数据官队伍的综合素质，引进数字化思维倒逼政府改革，释放数据要素红利。

一是推进数字沈阳建设。组织制订本地区或本部门的数字政府发展规划、数据战略规划和政策法规体系等，谋划和组织实施跨部门、跨层级、跨领域的融合型应用场景。

二是推动数据资源汇聚共享和安全防护。消除数据壁垒，建立和完善政务数据资源目录体系，强化政务数据资源的对接共享；推动建立大数据安全专家队伍，建立数据安全应急处置机制。

三是实施常态化指导监督。协调解决本地区、本部门信息化项目建设中的重大问题，并对数据治理运营、信息化建设等执行情况进行督导。

四是营造良好数字发展生态。加强人才队伍建设，积极培育大数据产业，发展数字经济新业态新模式，探索建立大数据交易机制，开展广泛宣传和推广工作等。

https://mp.weixin.qq.com/s/22aSV3QmvhbH-GPEroPJ7g

5、美商务部新规：未经审批禁止向中国分享安全漏洞

近日，美国商务部工业和安全局（BIS）正式发布了针对网络安全领域的最新的出口管制规定。主要是关于网络安全和漏洞信息的管控。

实际上，这次公布的新规定是 2021 年 10 月临时规定（征求意见稿）的最终确认。该规定将全球国家分为 A、B、D、E 四类，限制措施和严格程度逐步递增。中国被分在 D 类，即「受限制国家和地区」，E 类则为「全面禁运国家」。该规定对某些网络安全项目建立了新的控制方法，目的则是出于「国家安全和反恐考虑」。

同时，BIS 还增加了一项新的授权网络安全出口的例外情况。核心内容是授权这些网络安全项目出口到大多数目的地，但是上述提到的例外情况则不可以。BIS 认为，这些被

控制的项目可能被用于监视、间谍活动，或者其它以破坏等为目的的行为。

https://mp.weixin.qq.com/s/Y48iZ8RSqSpfpYlhHetnCA

6、泰国个人数据保护法正式生效，违规泄露隐私或可罚 500 万泰铢

近日，泰国全国新闻委员会发布公告称，泰国《个人数据保护法》（Personal Data Protection Act B.E.2562，简称 PDPA）将于 2022 年 6 月 1 日正式生效。

PDPA 是泰国制订的第一部用于管理和保护数据的法律，该法案适用于在泰国境内为泰国提供产品或服务而处理个人数据的实体。PDPA 规定了数据控制者和数据处理者（包括公共和私人实体）在处理、收集或披露个人数据之前，应如何获得数据主体的同意。此外，PDPA 规定数据主体有权要求访问其个人数据，并有权删除此类数据。数据主体也有权反对收集、使用或披露他们的个人数据。

https://mp.weixin.qq.com/s/Ig44H5oZnaX5aSJeQS4ohg

技术、产品与市场

1、Gartner：2025 年 60%的大型企业机构将使用隐私增强计算技术

Gartner 日前发布了 2022 年银行和投资服务行业的三大热门技术趋势，分别是：**生成式人工智能（生成式 AI）、自主系统和隐私增强计算。**这三项趋势将在未来两到三年内继续增长，推动金融服务机构的增长和转型。

隐私增强计算（PEC）能够保障在不可信环境中处理个人数据时的信息安全，而随着隐私和数据保护法的不断发展以及消费者的日益关注，这一点正变得越来越关键。隐私增强计算运用各种隐私保护技术使金融服务机构在从数据中获取价值的同时满足合规要求。

Gartner 预测，**2025 年 60%的大型企业机构将在分析、商业智能或云计算领域使用一种或多种隐私增强计算技术。**

数据在金融服务领域的各种分析、计算和数据变现工作中都起到了不可替代的作用。金融服务机构正越来越多地在欺诈分析、智能运维和数据共享等应用中采用 PEC。

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

2、首个“隐私计算安全需求”国际标准立项

近日，IEEE SA 标准委员会正式通过了“隐私计算安全需求”（Standard for Security Requirement of Privacy-preserving computation，P3169）国际标准的立项。该标准由蚂蚁集团主导，行业内专家共同参与，将对隐私计算技术本身潜在的安全隐患进行分析，并对隐私计算系统抵御的安全风险进行分级。目前，IEEE SA 已成立专门工作小组，蚂蚁集团牵头推进下一步实质性工作。

https://mp.weixin.qq.com/s/YVuCp1FG6kpHxG-NwSImRg

3、《数据防泄露（DLP）选型指南》报告发布

2022 年 5 月 31 日，在中国计算机学会抗恶劣环境计算机专业委员会指导下，由中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、安全牛和谷安研究院联合发起编制的《数据防泄露（DLP）选型指南》报告（以下简称为“报告”）正式发布。

数据防泄露产品以深度内容识别技术为核心，在数据存储、传输和使用过程中，发现并监控敏感数据，确保敏感数据的合规使用，防止主动或意外的数据泄露。DLP 产品可以帮助企业降低数据丢失和数据泄露的风险，但是由于 DLP 产品的多样化以及在功能上和性能上的复杂性，导致企业在

产品选型时面临挑战，甚至由于选型不当导致部署后无法有效地发挥效用。

报告通过调研发现：（1）88.31% 的受访企业部署了一种或多种数据防泄露产品，其中以终端防泄露产品为主，占比高达 80.52%，也有一半左右的企业采用了网络防泄露和邮件防泄露产品。（2）在选型阶段，目前用户最关注的几个方面包括 DLP 产品的功能、产品对网络和终端设备的影响、产品与环境的兼容性等。（3）企业在实际应用中，最关注的 DLP 产品功能包括内容识别、图像识别、对终端的安全控制、报警功能等。（4）超过半数的企业制定了数据防泄露管理制度和流程，作为技术工具使用的指引和基础，但是也有部分企业仅采用了 DLP 产品，并没有制定配套的数据安全管理制度，通过默认的流程或者仅凭管理人员的经验来进行日常的管理。

https://mp.weixin.qq.com/s/M6di_FGwiS1V9lrw5bFdxQ

4、《数字安全产业大数据白皮书》发布

近日，**数说安全、元起资本、腾讯安全联合发布《数字安全产业大数据白皮书》（以下简称《白皮书》）**，围绕安全产业发展趋势，拆解产业需求端和供给端规律和策略，探讨中国安全产业的发展格局与新路径。

《白皮书》指出，全球数字安全产业的发展并未受疫情太大影响。在安全领域投资活动中，中美依旧是最活跃的两个国家，成为全球数字安全发展版图的重要组成部分。

从我国安全产业需求端来看，2019 年-2021 年，我国各省份安全需求依旧增长明显。政府行业是安全采购项目的主力军，教育和医疗行业位列其次。安全采购项目的产品类别，依旧以防火墙、负载均衡、身份认证等传统产品为主，但随着《数据安全法》和《中华人民共和国个人信息保护法》落地，政企客户对于数据安全的关注度迅速提升，新型的数据安全解决方案成为关注重点。

针对供给端的补充，安全市场因其丰富的产品类型、不同需求层级的客户群体分布，致使我国数字安全市场呈现碎片化分布的竞争格局。安全公司的数量分布与省直辖市的 GDP 水平总体呈正相关关系。截止 2021 年底，我国安全公司共计 6164 家，北京市安全公司数量以 1927 家遥遥领先于其他省市。从安全产品资质来看，长三角区域的安全公司持有产品资质的比例要显著高于全国平均水平。

https://mp.weixin.qq.com/s/X20G5QrjryX75586tXREsg

5、支付赎金的医疗机构已经比过去多两倍

安全供应商 Sophos 通过对 31 个国家/地区的 381 名

IT 专业人员的采访，发布了《2022 年医疗保健中的勒索软件状况》报告。根据 Sophos 的最新数据，去年全球医疗保健组织 (HCO) 的勒索软件攻击同比激增 94%，选择向敲诈者付款的人数几乎是后者的两倍。

报告显示，去年三分之二的 HCO 都受到了勒索软件的攻击，高于 2020 年的三分之一。Sophos 声称，这种激增归因于勒索软件即服务在地下网络犯罪中的普及。然而，这也可能是 HCO 更愿意向攻击者付款的结果。大约 61% 的人在 2021 年支付了赎金，而一年前这一比例仅为 34%。高昂的修复成本、运营中断的影响，以及对医疗行业的攻击日益复杂，可以解释数据的飞跃。只有 2% 的受访者在支付了赎金后取回了所有数据。

https://www.infosecurity-magazine.com/news/healthcare-organizations-pay-ransom/

业界观点

1、杜广达：协同发力 构建数据安全产业生态

5 月 26 日下午，工业和信息化部网络安全管理局副局长杜广达在 2022 中国国际大数据产业博览会“数据安全论坛”上指出，要坚持统筹发展和安全，按照“成体系、有重点、分步骤”的工作思路，推动数据安全工作开好局、起好步。他表示，健全数据安全治理体系，要紧紧围绕重要数据保护这条主线，从制度机制、标准规范、技术能力等方面多措并举，构建重要数据识别报备、安全防护、风险评估、应急处置的安全治理闭环。

他强调，在构建数据安全产业生态方面，可以从五方面协同发力。**一是加强核心技术攻关**，面向国家数据安全重大需求，加快推进数据安全基础研究、核心技术和关键产品研发，提升产业供给能力。**二是加强创新载体建设**，大力推进数据安全产业园、重点实验室等创新载体建设，培育建立大中小企业梯次递进、协同发展的产业组织体系，打造技术、人才、资金等创新资源集成汇聚的策源地。**三是加强应用示范**，积极建设数据安全创新应用先进示范区，鼓励开展优秀实践案例选拔和示范推广活动，大力推进创新成果转化应用。**四是加强第三方服务**，积极培育第三方数据安全专业服务机

构，支持依法依规开展数据安全产品检测、风险评估、安全审计等服务。**五是加强宣传培训**，全面开展“会、展、赛、训”等系列宣传活动，促进产业供需对接和人才培养，加快提升监管人员和行业数据处理者的数据安全意识。

https://www.isc.org.cn/article/12669671364882432.html

2、肖亚庆：要顺应数字化发展趋势，坚定不移实施国家大数据战略

近日，工业和信息化部部长肖亚庆在 2022 中国国际大数据产业博览会上表示，数据是数字经济时代的关键生产要素，是国家基础性战略性资源，是推动经济社会高质量发展的重要引擎。对此，他指出四个建设路径。

一是加快建设数字基础设施。坚持适度超前建设，以建带用，以用促建，推动数字基础设施建设与应用场景协同发展。全面推进 5G 网络和千兆光网建设，加快工业互联网、车联网等布局，促进数据高效采集和传输。统筹布局数据与算力设施，加快建设国家工业互联网大数据中心，合理部署超级计算中心，打造若干国家大数据枢纽节点和区域中心集群。

二是着力拓展融合应用场景。围绕促进产业转型升级、提高政府治理效能、加快数字社会建设，开展大数据技术、产品和服务协同创新，补齐关键技术短板，构建稳定高效的

大数据产业链。以制造业数字化转型为引领，实施工业大数据价值提升行动，构建多层次工业互联网平台体系，培育一批专业化、场景化大数据解决方案，发展一批面向细分场景的工业 APP，推广一批基于数据驱动的新技术新业态新模式。

三是推进数据资源整合和开放共享。采好数据、管好数据、用好数据是大数据产业发展壮大的关键。工信部将加强部门联动、部省协同，加快数据确权、交易流通、跨境传输和安全等基础制度规范建设，探索多种形式的数据交易模式。鼓励互联网企业、电信运营商、工业企业等有序开放数据，实施数据管理能力国家标准。继续支持数据交易所建设，完善运营体系，培育一批数据交易服务商。

四是深化国际务实合作。工信部将坚定不移贯彻对外开放的方针，支持国内外大数据企业在技术研发、标准制定、产品服务、知识产权等方面深入合作，支持国内企业“走出去”开拓国际市场，支持跨国公司、科研机构在国内设立大数据研发中心、教育培训中心。工信部愿与各方一道，在多双边合作机制下，加强战略规划对接和政策沟通协调，携手营造公平开放的发展环境。

https://www.soeasytest.com/article-item-25.html

3、林念修：以产业互联网为主要增长点的“下半场”势头强劲，数字经济大有可为

在 2022 中国国际大数据产业博览会上，国家发展和改革委员会副主任林念修在以视频方式致辞时提到，我们将在党中央坚强领导下，以数字技术与实体经济深度融合为主线，以数字红利惠及更广大人民群众为根本目的，协调调动各方面力量，进一步做强做优做大我国数字经济。概括起来来说就是要重点做到“六个着力”：

一是着力夯实基础适度超前部署建设新型基础设施，完善信息基础设施建设，推进光纤网络扩容提速，5G 规模部署和融合应用，加快传统基础设施数字化改造，建设协同、先进、开放高效的创新基础设施体系。

二是着力激活潜力充分挖掘数据要素价值加快出台构建数据基础制度的政策文件统筹优化全国数据市场体系布局，进一步促进数据要素高效合规流通使用，落地全国一体化大数据中心布局，深入推进“东数西算”工程，抓紧在全国建设 10 个左右的数据中心集群。

三是着力推动转型促进实体经济高质量发展，全面深化大中小企业数字化改造升级，大力发展产业互联网平台，鼓励一二三产业融通发展，支持建设数字化转型促进中心，增强面向中小微企业、行业和区域的数字化转型服务能力。

四是着力稳链强链，大力推动数字产业创新发展，坚持产业攻关模式，不断创新方式方法，进一步深化关键核心技术攻关，聚焦重点数字产业，提升基础软硬件重要生产装备等自主供给能力和水平，支撑产业链供应链安全稳定。

五是着力强化保障，提高防范和抵御安全风险能力，强化关键信息基础设施保护，增强态势感知、威胁发现和协同处置等能力，推动网络和数据安全技术创新，培育富有竞争力的骨干企业，为维护国家网络安全提供技术和产业支撑。

六是着力优化环境，积极参与数字经济国际合作，健全完善数字经济治理体系，提升数字治理水平，积极参与国际数字经济议题谈判，开展双多边数字治理合作，推动“数字丝绸之路”走深走实，让数字经济合作成果惠及各国人民。

https://news.10jqka.com.cn/20220526/c639366767.shtml

4、曹淑敏：互联网企业要加大研发投入，让创新成为发展的核心竞争力

在 2022 中国国际大数据产业博览会上，中央网信办、国家互联网信息办公室副主任曹淑敏视频致辞指出，我国是数据资源大国，在数据资源开发利用初见成效，但我国数据领域还存在一系列问题，需要加快建立基础制度，推动数据开放开发和价值释放，助力高质量数字经济发展。对此，她提

出四点建议。

一是强化顶层设计，加快数字中国建设。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。

二是加快核心技术创新，实现高水平科技自立自强。互联网企业是网信领域的创新主体。进一步加大研发投入，让创新成为企业持续健康发展的核心竞争力。同时，加大对关键核心技术的协同攻关，营造充满活力的创新环境，建设互利共赢的产业生态。要继续强化企业创新主体地位，加强原创性、引领性科技攻关，构建开放创新生态，激发人才创新活力，助力实现高水平科技自立自强。

三是激活数据要素潜能，打造高质量数字经济。数据是数字经济的关键生产要素。我国是数据资源大国。近年来，我国数据资源开发利用初见成效，但仍需要加快建立完善数据权属、流通、交易等基础制度，推动数据开放开发和价值释放，助力高质量数字经济发展。

四是推动数据惠民便民，建设普惠包容数字社会。“十

四五”规划纲要，就“加快数字社会建设步伐”明确要求，提供智慧便捷的公共服务、建设智慧城市和数字乡村、构筑美好数字生活新图景。近年来，国家智能社会治理实验基地和数字乡村试点在探索数字条件下的社会治理和服务方面形成了一批可复制的宝贵经验。下一步，我们要继续聚焦教育、医疗等重点领域，发挥试点示范作用，推动数字化服务普惠。

https://finance.sina.com.cn/tech/2022-05-26/doc-imizirau4956379.shtml?finpagefr=p_114

5、数博会聚焦数据安全，专家探讨隐私计算“破局”困境

在 2022 中国国际大数据产业博览会上,开放数据要素、守护数据安全等话题备受关注。有专家表示，隐私计算作为新兴的数据流通安全技术，或可“破局”数据应用困境。

中国信息通信研究院副院长魏亮表示，当前，数据安全风险从相对静态交互向数据全生命周期迅速延展，数据保护重点也从相对静态的保障数据交互安全，向保障动态的数据要素流转安全转变。在此背景下，同态加密、差分隐私等隐私保护技术，为化解数据利用与数据保护之间的矛盾提供了有力支撑。

中国工程院院士邬贺铨进一步阐述了隐私计算的作用

和价值。他说，隐私计算是保护原始敏感数据不泄漏的前提下，实现数据分析与计算的一类技术集合。在隐私保护计算框架下，参与方的数据不出本地，实现“数据可用不可见、数据不动价值动”。

瑞莱智慧 CEO 田天表示，人工智能的发展路径能够为隐私计算的发展及破解种种难题提供参考和借鉴。从技术角度看，隐私计算能够解决数据的“链接”问题，为算法的持续进化提供数据补充；从落地角度看，基于人工智能的数据处理与分析能力，加上隐私计算的安全实现，能够在跨业、跨域数据融合的基础上，实现数据价值的深度挖掘与释放。

https://wcaqq.com/85911.html

数据安全事件

1、土耳其航空公司泄露 6.5TB 航班和机组人员信息

2022 年 5 月 31 日，土耳其航空公司 Pegasus Airlines 的 AWS 存储桶配置错误，泄露了 6.5 TB 数据。研究人员在 2 月 28 日发现了一个开放的存储桶,其中有约 2300 万份文档，涉及超过 300 万个飞行数据文件（如飞行图表、保险文件和机组轮班信息等),超过 160 万份机组人员的 PII 信息，以及 Pegasus 航空公司开发的电子飞行包(EFB)软件的源代码。目前，该存储库已被保护起来。

https://www.infosecurity-magazine.com/news/turkish-airline-exposes-flight/

2、哥斯达黎加公共卫生机构被 Hive 勒索软件攻击

2022 年 5 月 31 日，哥斯达黎加公共卫生服务网络上所有计算机系统于今晨受 Hive 勒索软件攻击后处于离线状态。目前调查仍在进行中，但哥斯达黎加政府机构表示，存储在 EDUS（统一数字健康）和 SICERE（集中税收系统）数据库中的公民健康和税务信息没有受到损害。

https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/

3、360 万+MySQL 服务器暴露在互联网上

据媒体 5 月 31 日报道，安全研究组织 Shadowserver Foundation 在上周进行的扫描中，发现超过 360 万台暴露的 MySQL 服务器使用默认端口 TCP 端口 3306。这些服务器在网上公开暴露并响应查询，可能成为黑客和勒索攻击者的目标。其中，有 230 万台通过 IPv4 连接，130 万台设备通过 IPv6 连接。最多的国家是美国，拥有超过 120 万台暴露的设备，其次是德国、新加坡、荷兰和波兰等国。不适当地保护 MySQL 数据库服务器可能导致数据泄露、破坏性的攻击、勒索攻击以及 RAT 感染。

https://www.bleepingcomputer.com/news/security/over-36-million-mysql-servers-found-exposed-on-the-internet/

4、数百个 Elasticsearch 数据库遭到勒索攻击

据报道，因为 Elasticsearch 数据库安全防护薄弱的缘故，导致其被黑客盯上，并被黑客用勒索信替换了其数据库的 450 个索引，如需恢复则需要支付赎金 620 美元，而总赎金打起来则达到了 279,000 美元。威胁行为者还设置了 7 天付款期限，并威胁在此之后赎金将增加一倍。如果再过一周没有得到报酬，他们说受害者会丢失索引。而支付了这笔钱的用户将得到一个下载链接，链接到他们的数据库转储，据称这将有助于快速恢复数据结构的原始形式。

https://www.freebuf.com/news/335077.html

5、南非总统的个人信贷数据泄露：该国已沦为“黑客乐园”

据南非媒体《星期日泰晤士报》报道，黑客团伙SpiderLog$窃取了南非现任总统 Cyril Ramaphosa 自 2000 年代在国内四大银行之一的贷款详细记录。SpiderLog$称，这批数据来自另一个名为 N4ugtysecTU 的黑客团伙，而后者曾于今年早些时候入侵信用报告机构 TransUnion，窃取了 5400 万消费者征信数据，几乎覆盖该国所有公民。泄露数据集中包含 Ramaphosa 本人的家庭住址、身份证号码及手机号码。

https://www.secrss.com/articles/42993

6、富士康墨西哥工厂遭勒索软件攻击

富士康公司确认其位于墨西哥的一家生产工厂在 5 月下旬受到勒索软件攻击的影响。富士康没有提供任何有关攻击者的信息，但勒索软件组织 LockBit 声称对此负责。根据富士康的通告，勒索软件组织 LockBit 在 5 月 31 日发起了攻击，威胁要泄露从富士康窃取的数据，除非富士康在 6 月 11 日之前支付赎金。

https://www.secrss.com/articles/43139

7、澳大利亚交易巨头 ACY 证券暴露 60GB 用户数据

2022 年 6 月 4 日，据外媒报道，一名安全研究员透露总部位于澳大利亚悉尼的贸易公司 ACY Securities (acy.com) 在网上公开了大量未经授权的用户和企业的个人和财务数据供公众访问。

本次事件是由于 ACY Securities 拥有的数据库配置错误所导致的。该数据库包含超过 60GB 的数据，这些数据在没有任何安全认证的情况下被暴露，这意味着任何对在此类平台上查找不安全数据库有一点了解的人都可以完全访问 ACY 的数据，这些数据包含 2020 年 2 月以来的日志，同时每秒都会更新最新的数据集。

https://www.hackread.com/australian-trading-giant-acy-securities-exposed-data/?web_view=true

8、Spirit Super 会员资料遭安全攻击而泄露

2022 年 5 月 30 日报道，Spirit Super 发生在 5 月 19 日的数据事件导致 2019 至 2020 年间约 50,000 条会员记录被泄露。据透露，当时 Spirit Super 工作人员的电子邮件帐户陷入广泛的网络钓鱼攻击活动。

Spirit Super 在一份声明中表示，这是一次伪装成官方通信的恶意电子邮件攻击期间的人为错误，这不是由于重大安

全控制漏洞或技术故障造成的，恶意电子邮件导致了工作人员的密码被泄露。该公司还表示，它认为有人未经授权访问了包含个人数据的邮箱，可能包含的个人数据类似于年度报表中的信息，包括姓名、地址、年龄、电子邮件地址、电话号码、会员帐号和会员余额等项目。

https://www.financialstandard.com.au/news/spirit-super-member-data-exposed-after-security-attack-179795303?&web_view=true

9、攻击者利用 GitHub 令牌窃取私人存储库数据

2022 年 6 月 1 日报道，GitHub 披露了上周的事件相关细节，黑客使用偷来的 OAuth 令牌，从私人仓库下载了数据。

OAuth（开放授权）是一个开放标准的授权框架协议，主要用于互联网上基于令牌的授权功能。它使得最终用户的账户信息能够被第三方服务所使用，如 Facebook 和谷歌。GitHub 分析说，攻击者使用了窃取的 OAuth 令牌对 GitHub API 进行认证，本次网络攻击是有选择性的，攻击者克隆了感兴趣的私人存储库。

https://mp.weixin.qq.com/s/2AGnX9F5TCtxmDJgX00-9g

10、制药巨头诺华遭受 Industrial Spy 勒索攻击

2022 年 6 月 3 日，据外媒报道，制药巨头诺华（Novartis）近期遭受了 Industrial Spy 勒索团伙的网络攻击。诺华表示，目前没有敏感数据受到损害。

Industrial Spy 勒索团伙于 6 月 3 日开始在其 Tor 勒索市场上以 50 万美元的价格出售据称从诺华公司窃取的数据。威胁参与者声称，这些数据与诺华公司的基于 RNA 和 DNA 的药物技术和测试有关，并且是“直接从制造厂的实验室环境中窃取的”。由于要出售的数据量很少，尚不清楚这是威胁行为者窃取的全部数据，还是他们以后还有更多数据要出售。

https://www.bleepingcomputer.com/news/security/novartis-says-no-sensitive-data-was-compromised-in-cyberattack/