全球数据安全观察

总第 89 期 2022 年第 17 期

（2022.05.16-2022.05.22）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、银保监会发布《银行保险机构消费者权益保护管理办法（征求意见稿）》，信息安全权受关注

5月19日，银保监会发布《银行保险机构消费者权益保护管理办法（征求意见稿）》（以下简称《管理办法》），向社会公开征求意见。《管理办法》共8章，56条。《管理办法》第二章第十二条要求，银行保险机构应当**建立消费者个人信息保护机制，完善内部管理制度、分级授权审批和内部控制措施，对消费者个人信息实施全流程分级分类管控**。

《管理办法》第六章特别强调保护消费者信息安全权。银行保险机构处理消费者个人信息，应当坚持“合法、正当、必要”原则，切实保护消费者信息安全权。银行保险机构收集消费者个人信息应当向消费者告知收集、使用的目的、方式和范围等规则，并经消费者明示同意。消费者不同意的，机构不得因此拒绝提供不依赖于其所拒绝授权信息的金融产品或服务，不得采取变相强制、违规购买等不正当方式收集消费者个人信息。银行保险机构应在消费者授权同意的基础上与合作方处理消费者信息，与合作机构的协议中应约定数据保护责任、保密义务、监督、处罚、合同终止和突发情况下的应急处置条款。合作过程中，应通过加密传输线路、

安全隔离、数据加密、权限管控、监测报警等方式，严格控制合作方行为与权限，开展数据分析等方面合作应使用脱敏后的数据，防范数据滥用或泄露风险。银行保险机构应督促和规范与其合作的互联网平台企业有效保护消费者个人信息，未经消费者授权同意，不得在不同平台间传递消费者个人信息。不得利用痕迹数据对消费者开展未经授权的营销活动。银行保险机构处理和使用个人信息的业务或信息系统,遵循权责对应、最小必要原则设置访问、操作权限,落实授权审批流程，实现异常操作行为的有效监控和干预。银行保险机构应加强从业人员行为管理，禁止违规查询、复制、下载、储存消费者个人信息，不得超出自身职责和权限非法处理和使用。

https://mp.weixin.qq.com/s/vOQuBF03kB1LI2BBVVavXw

2、《关于推进实施国家文化数字化战略的意见》印发，强化文化数据要素市场交易监管

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》提出了 8 项重点任务。一是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。二是夯实文化数字化基础设施，依托现有有线电视网络设施、广电 5G 网络和互联互通平台，形成国家文化专网。三是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。四是鼓励和支持各类文化机构接入国家文化专网，利用文化数据服务平台，探索数字化转型升级的有效途径。五是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。六是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。七是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。八是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。

《意见》要求，**在数据采集加工、交易分发、传输存储及数据治理等环节，制定文化数据安全标准，强化中华文化数据库数据入库标准，构建完善的文化数据安全监管体系，完善文化资源数据和文化数字内容的产权保护措施**。加快文化数字化建设标准研究制定，健全文化资源数据分享动力机制，研究制定扶持文化数字化建设的产业政策，落实和完善财政支持政策。

https://mp.weixin.qq.com/s/XRXhMKwv_vdL1EIwNOZiZA

3、北京市通信管理局开展2022年电信和互联网行业网络与数据安全检查

5月19日，北京市通信管理局发布关于开展2022年电信和互联网行业网络与数据安全检查的通知。本次检查工作检查对象为提供公共互联网网络信息服务的基础电信企业、域名注册服务企业、云平台服务提供商、APP运营企业、车联网平台企业、工业互联网平台和标识解析节点企业等。重点检查相关网络运行单位的关键信息基础设施和重要网络单元及承载的信息系统，包括但不限于：通信网络基础设施、公共云服务平台、域名服务系统、工业互联网平台、标识解析系统、车联网应用服务平台、网约车信息服务平台等。

检查内容包括**网络安全管理制度和保障体系建设落实情况、通信网络安全防护工作落实情况、数据安全保护落实情况、个人信息保护工作情况、工业互联网企业网络安全防护情况**。

据通知安排，自通知发布之后到6月15日前为自查自纠期，6月16日起至9月30日将进入重点抽查期，对检查过程中发现的问题将对企业进行整改问责。

https://mp.weixin.qq.com/s/5U04W9TGFt8zVZEHnqruOg

4、《大连市数字政府建设“十四五”行动方案》出台，完善数据标准体系，深化数据治理

近日，《大连市数字政府建设“十四五”行动方案》（以下简称《行动方案》）正式出台，明确了“十四五”期间大连市政府数字化转型全面发展的目标和路径。《行动方案》以全面贯彻新发展理念，聚焦数字政府建设，坚持全市统一架构体系、统一技术标准和统一数据管理，通过信息技术与政府业务广泛深度融合，推进政府数字化转型发展，打造政务业务“一网协同”、政务服务“一网通办”、社会治理“一网统管”的数字政府新格局，提升社会治理能力现代化水平，促进营商环境优化和经济社会发展，推动“两先区”建设和高质量发展新突破。

《行动方案》根据数字政府层级架构具体分解工作任务。基础设施建设方面：全面掌握政府自建机房基础设施情况，利用现有基础设施资源，提升政府数据中心一体化算力，由各部门分散运维向市大数据中心统一运维转变；数据支撑建设方面：**健全完善数据资源共享交换通道，建立动态更新的数据挂载机制，完善数据标准体系，深化数据治理**；应用支撑建设方面：着力建设综合应用支撑平台，作为全市电子政务系统总入口，采用单点登录方式集成各委办局业务系统和各区市县自建个性化系统；重点应用建设方面：加快推进政

府运行“一网协同”，整合推广全市既有资源和优秀应用，升级改造政务服务“一网通办”，探索开展惠企政策主动推送和“免申即享”，推动提升社会治理“一网统管”，实现“一屏观全城”“一屏管全城”。

https://mp.weixin.qq.com/s/4MoKtKSUsJEQqq4B61hfvg

5、宁夏 5 部门联合发布：《关于进一步规范全区政务信息化项目商用密码应用和安全性评估的通知》

近期，宁夏密码管理局、自治区党委网信办、发改委、公安厅和财政厅等 5 部门联合印发《关于进一步规范全区政务信息化项目商用密码应用和安全性评估的通知》(宁密局发〔2022〕1 号)，持续推动和规范政务信息化项目商用密码应用与安全性评估工作。

《通知》强调，各地各部门要高度重视政务信息化项目的商用密码应用和安全性评估工作，强化底线思维和风险意识，贯彻总体国家安全观，切实履行政治责任和法律责任，严格按照《中华人民共和国密码法》的要求，依据相关政策法规和标准规范，在电子政务外网等非涉密信息系统中合规、正确、有效使用商用密码，保障网络与信息安全。

《通知》要求在项目规划阶段，应制定密码应用方案，并委托评估机构对方案开展密码应用安全性评估，未通过密

评的密码应用方案，不得作为密码保障系统的建设依据；项目建设完成后，应委托评估机构开展密码应用安全性评估。结论为“符合”或“基本符合”的密码应用安全性评估报告是项目验收必备材料；信息系统投入运行后，项目建设单位应委托评估机构每年对系统开展密码应用安全性评估，确保密码保障系统正确有效运行。

https://mp.weixin.qq.com/s/DigWkR3J4Yv174OixACCXw

6、全国首家数据资源法庭设立！覆盖个人信息侵犯、数字资源窃取、监管失职等案件

5 月 18 日上午，温州市瓯海区人民法院数据资源法庭正式揭牌设立。据悉，这是经浙江省高级人民法院同意、中共浙江省委机构编制委员会办公室批准，国内设立的首个以受理数据资源案件为核心业务的专业法庭。

数据资源法庭实行刑事、民事、行政‘三合一’归口审理模式，换言之，只要是涉及数据资源的案件，都可以在此审理。具体案件管辖范围包括：严重侵害个人信息、商业秘密、保密商务信息等合法权益刑事案件以及数据监管职务犯罪相关案件；不当侵害包括个人信息、商业秘密、保密商务信息等在内的与数据资源权益相关的侵权责任纠纷和合同纠纷民事案件；网络不正当竞争和数据资源权属纠纷等知识

产权案件；涉及数据资源行政许可、信息公开、行政处罚、行政监管等行政案件和非诉行政执行案件。

数据资源法庭在履行审判职能外，还将开展数据资源保护普法宣传工作，助推企业合规建设，引导企业提升保密意识，完善数据资源保护工作，在经营过程中合法合规收集、使用、交易数据，避免侵害数据资源利用人和其他相关人的合法权益；加强对数据资源保护工作的调研，结合数据资源法庭运行情况，针对维护企业及国家数据资源安全、数据资源案件审理难点、数据资源立法保护工作等方面开展调研，努力为数据资源保护立法提供温州经验。

https://mp.weixin.qq.com/s/C7C85Ckqq_UmTF9W7i1hsw

7、美国第五部州隐私法来了！照片、视频不属于生物特征数据

据美国康涅狄格州议会官网消息，近日，在获得康涅狄格州立法机构表决通过十几天后，《康涅狄格州消费者隐私法》（下称《隐私法》）经州长签署后正式通过，将于明年7月1日起生效。继加利福尼亚州、弗吉尼亚州、科罗拉多州和犹他州出台隐私法后，康涅狄格州（下称“康州”）成为第五个出台隐私法的大州。

在《隐私法》中，“生物特征数据”被定义为通过自动

测量个人的生物特征而产生的数据，如指纹、声纹、视网膜、虹膜或其他用于识别特定个体的独特生物特征。然而，数字或实物照片、音频或视频以及由其产生的任何数据不被包括在内——除非这些数据是为识别特定个人而生成。

https://mp.weixin.qq.com/s/r4ZLEgf_J_sz8BIB1xQF0g

技术、产品与市场

1、约两成 App 存在违规收集个人信息风险，影响超两亿用户

近日，奇安信病毒响应中心发布了 2022 年第一季度**《App 违规收集个人信息风险分析报告》**（简称《报告》），对**近 30 万个**全国应用市场新增 App 活跃样本个人信息收集情况进行了详细的分析。

《报告》显示，APP 违规收集个人信息的现象仍然十分普遍，平均每 5 个 App 中，就会有一个存在个人信息收集方面的违规风险。其中，“无提示收集个人信息”风险和“高频次收集个人信息”问题最为显著，也是本次报告关注的重点问题。个别 APP 平均每 0.7 秒就会无提示收集一次用户个人信息，可谓是对用户个人信息的“不间断”的收集。

部分存在违规收集个人信息风险的 APP 社会影响面巨大，仅下载量排名靠前的 24 款 APP 就至少影响国内超过 2 亿用户。网上购物、生活休闲、办公商务等常用 APP 的违规风险问题最为突出。

八成以上的违规个人信息收集行为实际上是由于 APP 集成了某些不规范的第三方 SDK，或者是没有对第三方 SDK 收集个人信息的行为进行声明造成的。作为软件开发者，在

集成第三方 SDK 时，应当遵守相关法律法规，拒绝使用存在违规风险的 SDK，从而努力规避自身的违规风险。

https://www.wangan.com/p/7fy7f606a51ec1f1

2、360EDR：数字时代新终端防御利器

近日，**360 政企安全集团联合 Gartner 在全球发布了 EDR 白皮书——《数字时代 EDR 技术发展趋势》**。白皮书指出：面向数字时代的 EDR 技术应该致力于真正解决终端所面临的各类高级威胁问题，以云端能力为核心，以安全大数据、威胁情报、高精度异常数据采集等核心技术为支撑，有效规避传统终端安全产品（EPP）检测技术的弊端，打造高维度的威胁检测对抗能力，做到事前预防、事中检测和事后修复。

基于多年实战经验积累，360 政企安全集团以体系化作战/对抗/攻防思维的新战法为指导，打造了一套以云端安全大脑为核心的数字安全能力框架。在此框架下，构建了面向未来的 EDR 方案——360 终端检测响应系统（简称“360EDR”）。360EDR 依靠云端安全大脑在数据、情报、专家等方面的赋能，以及核心安全大脑“运营商”级的分析算力支撑，构建了“云地一体化”架构，以低成本、高效率、易部署的优势满足互联网和隔离网场景下的安全防护需求。

http://www.techweb.com.cn/news/2022-05-16/2890905.shtml

3、2021 年赎金需求激增 45%

根据 Group-IB 的数据，2021 年的平均赎金需求为 247,000 美元，比上一年增加了 45%，大多数威胁参与者都试图通过双重勒索手段强制付款。

这家安全供应商称勒索软件的持续上升归因于暗网上初始访问代理和勒索软件即服务产品的扩散。该报告认为，更复杂的威胁使受害者更难恢复：攻击造成的平均停机时间同比从 18 天增加到 22 天。

Group-IB 还表示，去年 63% 的攻击使用数据盗窃和威胁泄露作为强制付款的方法。Lockbit、Conti 和 Pysa 在向泄露网站发布数据方面最为激进。然而，引起人们注意的是两个新来者 Hive 和 Grief——按发布到泄密网站的受害者人数计算，它进入了勒索软件团伙的前 10 名名单。前者向 MediaMarkt 索要 2.4 亿美元的巨额赎金，这是今年和有史以来最大的一笔赎金

https://www.infosecurity-magazine.com/news/ransom-demands-surge-45-in-2021/

4、数世咨询：API 安全研究报告 2022

API 逐渐形成了自身的技术和经济生态，在全球范围内被采纳，是公认的数字时代的价值链接基础。

API 已经成为网络应用流量最重要的出入口，通过攻击 API 来破坏信息系统和窃取数据，将成为数字时代黑产活动最集中的方向之一。

事实不断证明，传统的 API 网关或 WAF 的防护方式已无法再满足企业的 API 安全需求，数字时代需要专注于 API 的安全解决方案。

数字时代的 API 安全产品应该以 API 安全生命周期为线索，在解决协议覆盖、资产梳理以及攻击检测的基础上，通过深度学习的能力，精准描绘出业务逻辑和数据流向。通过对业务流量和数据的学习，整合安全资源，达到攻击预防、攻击阻断以及敏感数据泄漏防护的目的，最终实现 API 运行时防护的安全状态。

企业开展 API 安全建设，可以优先考虑以收敛、整合、智能、自动为核心的安全框架。

https://mp.weixin.qq.com/s/evxosmNr6NtYceeu-iuFUg

5、《中国数据交易实践趋势报告》发布

专家认为，具有政府背景的大数据交易所若能为企业数

据安全提供合规科技、风险评估与安全认证，并为个人信息提供可交易的规则，企业将会有较大动力进场内交易。

报告指出，当下数据交易面临的部分难题有:

（1）核心技术创新不足支撑不够：在数据安全保障、权属界定、价值挖掘、创新应用等核心领域，应用 AI 区块链、隐私计算等技术创新依然不足;

（2）缺乏有效治理，阻碍数据流通：目前政府和互联网平台汇聚大量高价值数据，但伴随“大量”而来的是“混乱”“无序”、尤其是政府数据普遍缺乏有效治理，不能提供持续、多源的、标准化的数据资源，阻碍数据流通。

报告针对以上问题给予的建言有:

（1）推进数据市场标准化，降低流通壁垒与成本;

（2）完善数据交易市场层级结构，培育生态体系。

https://mp.weixin.qq.com/s/edF-Fp7nVtUiQ8u4FjZBMw

业界观点

1、个人信息保护与数据安全治理探讨

5 月 13 日，第五届中国数据安全治理高峰论坛——个人信息保护与数据安全治理论坛在线上成功召开，多位专家聚焦个人信息保护现状、数据安全治理发展及创新成果等热点方向发表观点。

其中，刘文强在致辞中指出，个人信息保护与数据安全治理发展应注重三个方面的问题：一是创新探索，为保障数字经济的健康发展，亟须探索出一条安全治理的有效路径；二是集智攻关，要加强产学研合作，建立研究机构与相关数据处理主体的联动机制，运用研究技术的科研能力，结合企业技术积累和服务体系，开展数据治理的示范应用；三是久久为功，国内头部企业要发挥示范引领作用，不断增强网络安全防护能力及数据安全保障水平，切实有效防范各类风险。

此外，赛迪研究院网络安全所副所长闫晓丽提出，需要通过加强数据安全监督管理、建立平台企业数据业务有序发展机制、强化数据安全宣传教育三方面来进一步提升数据安全和个人信息保护意识，改善我国数据安全治理现状。

https://finance.eastmoney.com/a/202205172381938023.html

2、观点：在华外企需走出舒适区适应本地化监管

2022 年 4 月 21 日，美中贸易全国委员会（USCBC）在北京发布题为《美国公司如何接近中国的数据、隐私和网络安全制度》的报告（以下简称报告）。报告显示美企对数据和隐私保护制度有六方面关注和担忧:

（1）58%的公司认为，对跨境数据流动的限制不同程度地损害了外国企业在中国的运营和竞争力，因为这些企业采用的是全球设施、统一运营的模式，需要数据的无缝链接。

（2）与数据出境限制问题相伴生，54%的公司担心数据本地化要求会显著增加它们在中国的运营成本，同时从其全球 IT 基础设施中断开与公司中国业务的联结。

（3）担心中国对收集的一定数量个人信息采取与重要数据相同的限制和控制，这一趋势可能会影响拥有大量个人信息的公司，尤其是面向消费者的公司。

（4）56%的会员公司强调中国数据和隐私制度某些方面的模糊性是一个问题。

（5）认为中国隐私立法与其他市场标准（譬如欧盟的《通用数据保护条例》）之间最大的差异之一是要求“单独同意”。

（6）在接受采访的成员中，那些在特定行业，譬如汽车、酒店、医疗保健和金融服务领域工作的企业表示，新的数据

和隐私规则带来了一系列独特的挑战，这些挑战超出了他们与监管机构的传统交往经验，进一步使它们在网络安全和数据合规性方面工作复杂化。

对此，在华美企目前采取了四项应对措施，包括修改政府事务策略、镜像公司数据、调整结构和制定新计划、评估数据存储实践等。

对于报告中客观公正的观点或对近期中国数据、隐私保护和网络监管环境产生诸多不适感和不安感，专家建议：重点推进数据分类分级、数据出境管理、数据安全评估等关键制度实施细则；研究制定重要数据识别、保护要求、风险评估等配套指引，完善重要数据全流程安全保障体系；中国的法治建设速度是超出许多人想象的，可享受的立法空白红利空间只会越来越小，外企应主动去理解、去调整，早点走出过去的舒适区，从自己的超额利润中拿出一部分作为网络安全成本支出，以适应中国相关的监管要求。

https://www.secrss.com/articles/42656

3、王一鸣：加快推进中小企业数字化转型

当前，我国数字化转型由消费领域向生产领域扩展。中小企业占我国企业数量 90%以上，中小企业数字化转型是产业数字化的关键点，也是难点。

全国政协委员，国务院发展研究中心原副主任王一鸣突出以下建议：

创新支持中小企业数字化转型方式，解决不愿转问题。鼓励有条件的龙头企业、链主企业开放数据资源，提升上下游协同效率，带动中小企业融入数字化应用场景和产业生态。

为中小企业数字化转型提供示范引领，解决不敢转问题。依托“专精特新”中小企业，推进研发设计、生产制造、经营管理、销售服务等全流程数字化，树立具有行业代表性的数字化转型标杆。

完善中小企业数据安全监管体系，解决不想转问题。制定和完善企业数据安全的法规条例，保障中小企业数据资产权益和涉及商业秘密的数据安全。健全完善数据安全监管体系，提高监管能力和技术水平。

加强中小企业数字化人才培养，解决不会转问题。依托高等院校开办面向中小企业的培训项目，为中小企业培育一批既懂生产工艺又熟悉信息网络技术的专业人才。

http://jyzz.zgzx.com.cn/2022-05/18/content_9862161.htm

4、苗圩：多措并举推动数据确权

全国政协经济委员会副主任苗圩表示，产权界定清晰、权责明确，数据才能共享流通。因此建议：

明确数据确权的基本原则。充分把握数据发展规律和特点，是推动数据确权的重要遵循。要坚持分类分级，兼顾不同类型数据的管理和使用需求；要坚持安全发展，处理好发展与安全的关系，探索更加精准的数据确权。

积极构建数据确权基本框架。应妥善处理国家数据主权、国家安全、企业数据产权和个人信息保护之间的关系，框架设计要考虑三个重点：一是明确公共数据的公有性质，所有权归国家所有；二是厘清数据所有权、使用权、运营权、收益权等权利，形成体系化的数据权利束；三是强化数据权利司法保护，依法保护权利人对数据控制、使用、处理、受益等合法权益。

充分利用技术手段推动数据确权。利用多方安全计算等技术，在不转移原始数据的前提下实现对数据的开发利用，推动数据所有权和使用权分离，实现数据可用不可见。

https://www.tmtpost.com/nictation/6114310.html

5、刘尚希：数字经济治理要有风险整体观

从风险视角来观察，安全、发展都是风险问题。不安全，是风险；不发展、发展慢更是风险。全国政协委员，中国财政科学研究院院长刘尚希认为从风险整体观来看，当前面临以下问题，并分别提供了相应的建议：

一是进一步做好统筹发展和安全工作。这既有认识不到位的问题，也有体制机制问题。一方面，从局部看，即从部门职责看，通过规范和强监管，数字安全风险小了；另一方面，从全局看，即从国际竞争力来看，数字发展风险上升了。

二是数字革命带来的大趋势是虚拟化。从本质上看，数字技术都是虚拟化技术，让受到物理时空限制的经济活动转移到虚拟时空中实现，经济效率由此得以提高。走向数字制造，同样也要实现虚拟化、无人化和智能化。数字化与工业化一样，有其自发生成的发展顺序，政府应顺势而为。

三是资本和研发创新是一体两面，没有资本的跟进，就不会有研发创新。种子基金、天使投资、风险投资和股权基金等不同资本形态，对应着研发创新的不同阶段，资本是研发创新的孵化器和产业生态形成的助推器。

http://jyzz.zgzx.com.cn/2022-05/18/content_9862154.htm

数据安全事件

1、谷歌因违反 GDPR 被西班牙监管机构处以千万欧元罚款

2022 年 5 月 18 日，西班牙数据保护局（AEPD）宣布对 Google 提起的诉讼作出裁决，认定 Google 在未经授权的情况下，向第三方转移个人数据并妨碍用户行使删除权，决定依据 GDPR 第 6 条和第 17 条对其处以 1000 万欧元的罚款。

根据 AEPD 的公告，Google 作为数据的控制者，需要在美国对用户的个人数据进行分析处理。但是 AEPD 发现 Google 在向第三方 Lumen Project（以下简称 Lumen）传输数据时，向其发送了 Lumen 索要的包括个人身份、Email、给出的原因以及 URL 地址等个人数据。AEPD 认为，以上个人数据被转移到另一个可公开访问的数据库中，并可通过网站传播，导致“行使删除权的目的在实践中受到挫折”。

https://www.secrss.com/articles/42599

2、赞比亚央行遭勒索软件攻击，部分系统中断服务

2022 年 5 月 19 日安全内参消息，据彭博社报道，赞比亚银行表示，**不会向 Hive 勒索软件团伙支付赎金**。此前 Hive 团伙对该银行发动攻击，但**系统受到的损害相当有限。银行的部分信息技术应用中断服务，包括外汇管理局监控系统和**

网站，部分测试数据也可能被泄露。

https://www.secrss.com/articles/42574

3、芝加哥公立学校的供应商遭到勒索攻击，50 万学生的信息泄露

2022 年 5 月 21 日消息，芝加哥 495448 个学生和 56138 个员工的数据已经泄露。泄露事件源于芝加哥公立学校（CPS）的供应商 Battelle for Kids 在 12 月遭到了勒索攻击，导致其学校系统中的存储数据泄露。该公司与 267 个学校系统合作，项目涉及超过 280 万学生。此次泄露了 2015 至 2019 学年的数据，包括学生的个人信息和分数，以及员工的个人信息等。尽管 CPS 要求该公司立即通知数据泄露情况，但其在超过 4 个月后才披露了违规行为。

https://www.secrss.com/articles/42574

4、Conti 勒索软件关闭运营，成员迁移到更小型的勒索操作

2022 年 5 月 20 日报道，臭名昭著的 Conti 勒索软件团伙已经正式关闭了他们的运营，基础设施已经下线，团队领导人被告知该品牌已经不复存在。这个消息来自 Advanced Intel 的 Yelisey Boguslavskiy，他今天下午在推特上说该团伙的内部基础设施已经关闭。

虽然面向公众的 Conti 新闻数据泄漏和赎金谈判网站仍然在线，但成员用于执行谈判和在其数据泄漏网站上发布"新闻"的 Tor 管理面板现在已经关闭。

虽然 Conti 在与哥斯达黎加的信息战中关闭可能看起来很奇怪，但据称 Conti 进行了这次非常公开的攻击以创建一个实时操作的假象，而 Conti 成员慢慢迁移到其他更小的勒索软件操作。

https://www.cnbeta.com/articles/tech/1271855.htm

5、美国医疗保健公司 Omnicell 称其系统遭到勒索攻击

2022 年 5 月 17 日报道，美国医疗保健公司 Omnicell 遭到了勒索攻击。Omnicell 在 5 月 9 日在向美国证券交易委员会提交的文件中表示，勒索攻击发生在 5 月 4 日，其部分内部系统受到影响。此外，该事件可能导致该公司的商业机密或其它知识产权的丢失，以及公司员工、客户和供应商等人的个人信息泄露。截至 5 月 17 日，Omnicell 仍未在其网站上发布有关违规的正式通知。

https://www.cnbeta.com/articles/tech/1271855.htm

6、日经新闻亚洲子公司遭勒索软件攻击

2022 年 5 月 20 日报道，据出版巨头日经新闻（Nikkei）

透露，该集团在新加坡的总部遭到勒索软件攻击。

“5 月 13 日我们首次发现了对服务器的未经授权访问，随后已启动内部调查。”在公司发布的一份新闻稿中这样写道，“日经亚洲集团第一时间关闭了受影响的服务器，并采取了其他措施将影响降到最低。”

日经新闻补充表示，目前正在调查攻击者是否访问了可能存储在受影响服务器上的客户数据，“受影响的服务器可能包含客户数据，日经目前正在确定攻击的性质和范围”。截至目前，在调查勒索软件攻击时都没有发现数据泄露的证据。

https://www.bleepingcomputer.com/news/security/media-giant-nikkei-s-asian-unit-hit-by-ransomware-attack/

7、制药巨头遭受数据泄露，影响了 360 万客户

2022 年 5 月 18 日，据外媒报道，药房零售商 Dis-Chem 遭受数据泄露事件，未经授权的一方设法访问了数据库的内容，360 万客户的个人详细信息数据可能泄露。

Dis-Chem 在一份声明中表示，它与第三方服务提供商和运营商签订了某些托管服务的合同，这些服务为 Dis-Chem 开发了数据库。它补充说，该数据库包含“Dis-Chem 提供的服务所需的某些类别的个人信息”。

随后的调查显示，该事件总共影响了 3,687,881 名数据主体，并且访问了以下个人信息：名字和姓氏、电子邮件地址;和手机号码。

https://www.infosecurity-magazine.com/news/pharmacy-giant-data-breach/

8、2250 万马来西亚人的数据在暗网以 10,000 美元价格出售

2022 年 5 月 18 日，据外媒报道，据称，1940 年至 2004 年间出生的 2250 万马来西亚人的信息从国民登记局（NRD）被盗。

当地科技门户网站 Amanz 报道称，该数据库大小为 160GB，在暗网上以 10,000 美元（13,846 新元）的价格出售。卖家声称这是一个扩展的数据库，在截图中显示了姓名、电子邮件、手机号码和地址等详细信息。

https://www.theedgemarkets.com/article/data-225-million-malaysians-allegedly-stolen-nrd-being-sold-over-us10000-each

9、ICCL 揭露“最大规模数据泄露”，上网记录和位置每天被分享七百次

近日，爱尔兰公民自由委员会（Irish Council for Civil

Liberties，ICCL）公布了一份报告，对其认定的一起“史上最大规模数据泄露事件”进行了披露。

报告显示，如谷歌、微软等公司会利用实时竞价系统将用户的网络浏览记录和地理位置信息提供给广告商，以便广告商选择有潜在用户浏览的网页精准投放广告。在美国其每天分享上述用户信息 2940 亿次，平均每人被曝光 747 次；在欧洲每天分享 1970 亿次，平均每人被曝光 376 次，并且“没有任何办法可以控制这些数据的用途”。

报告推测，总体而言，美国网络用户的网络浏览记录和位置信息每年被追踪和共享 107 万亿次，欧洲每年为 71 万亿次，并称这些用户数据会被发送至全球各地的公司。值得一提的是，报告强调上述数据都十分保守，因为此次 ICCL 仅选择了在线广告生态系统的“巨头”之一谷歌参与统计，并未关注脸书和亚马逊。

https://mp.weixin.qq.com/s/HnDUoWbV8e4V1gPZso--pA

10、美国德克萨斯州保险部(TDI)泄露 180 万公民的信息

2022 年 5 月 18 日，美国德克萨斯州保险部(TDI)公开了有关 1 月份发现的数据泄露事件的更多信息。此次事件源于 Web 应用中存编程代码错误，导致受保护区域可以被访问，涉及超过 180 万公民的信息。经过调查确定，在 2019 年 3 月

至 2022 年 1 月期间，与工人赔偿要求有关的信息可能被外部人员访问，包括姓名、地址、出生日期、电话号码、社会安全号码以及有关伤害和工伤赔偿的信息。该机构此前表示，已经向受影响的人发送通知。

https://therecord.media/texas-data-breach-exposes-personal-information-of-1-8-million-people/