全球数据安全观察

总第 139 期 2023 年第 20 期

（2023.06.26-2023.07.09）

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、关于调整《网络关键设备和网络安全专用产品目录》的公告

7月3日，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门更新了《网络关键设备和网络安全专用产品目录》，《关于发布〈网络关键设备和网络安全专用产品目录（第一批）〉的公告》（2017年第1号）中的网络关键设备和网络安全专用产品目录同步废止。

https://wap.miit.gov.cn/jgsj/waj/wjfb/art/2023/art_9080a8689c58416eaf56f88649c242d3.html

2、民航局发布《关于落实数字中国建设总体部署 加快推动智慧民航建设发展的指导意见》

近日，中国民用航空局发布《关于落实数字中国建设总体部署 加快推动智慧民航建设发展的指导意见》，指导行业全面推动数字化转型、智能化应用、智慧化融合，在“筑牢民航数字安全屏障”部分，意见提出要增强数据安全保障能力：建立数据分类分级保护基础制度，按照“谁管业务，谁管业务数据，谁管数据安全”的原则，完善数据安全工作体系，健

全数据目录管理、监测预警、全生命周期管理等机制，加强数据安全应急处置。

https://www.gov.cn/zhengce/zhengceku/202307/content_6889672.htm

3、粤港澳大湾区数据跨境流动合作备忘录签署

6月29日，国家互联网信息办公室与香港特区政府创新科技及工业局签署《关于促进粤港澳大湾区数据跨境流动的合作备忘录》，在国家数据跨境安全管理制度框架下，建立粤港澳大湾区数据跨境流动安全规则，促进粤港澳大湾区数据跨境安全有序流动，推动粤港澳大湾区高质量发展。

https://www.cnbayarea.org.cn/news/focus/content/post_1076032.html

4、金融监管总局：加强第三方合作中网络和数据安全管理

日前国家金融监督管理总局向各地方银保监局、银行、保险、理财公司等机构下发了《关于加强第三方合作中网络和数据安全管理的通知》。国家金融监督管理总局要求，银行保险机构应强化“服务外包、责任不外包”的主体意识，切实承担数据安全主体责任，统筹管理科技风险，压实外包服务商安全责任，提升整体防控水平。

https://www.secrss.com/articles/56038

5、 北京市政府印发《关于更好发挥数据要素作用进一步加快发展数字经济的实施意见》

近日，中共北京市委北京市人民政府印发《关于更好发挥数据要素作用进一步加快发展数字经济的实施意见》。作为北京版“数据二十条”，该意见提出要发展数据安全服务业，支持企业开发数据安全评估、资产保护、数据脱敏、存储加密、隐私计算、检测认证、监测预警、应急处置等产品和服务；并从加强数据分类分级保护、完善数据安全技术体系、支持第三方几口开展数据安全和合规性的评估和审查、建立实施数据安全管理认证制度等方面明确强化数据安全和治理的路径。

http://jxj.beijing.gov.cn/zwgk/zcwj/bjszc/202307/t20230707_3157870.html

6、北京发布首个自动驾驶示范区数据分类分级管理细则

6 月 30 日，北京市高级别自动驾驶示范区工作办公室正式发布《北京市智能网联汽车政策先行区数据分类分级管理细则（试行）》，在国家数据分类分级保护制度下，深入结合示范区车路云一体化数据管理实践经验与企业安全发展诉

求，通过引导明确数据分类策略，定量数据定级方法并提供实操样本案例，有效推动形成依法规范、协同建设、共享红利的示范区数据安全发展模式。

http://kfqgw.beijing.gov.cn/zwgkkfq/yzttkfq/202307/t20230701_3152556.html

7、《深圳市数据产权登记管理暂行办法》发布

7 月 4 日，深圳市发展和改革委员会发布《深圳市数据产权登记管理暂行办法》，对登记申请人及登记主体、登记机构、登记行为等提出规范要求，并规定登记机构应当建立保护数据传输、存储和使用安全的基础设施，加强防攻击、防泄漏、防窃取的监测、预警、控制和应急处置能力建设，制定数据安全事件应急预案，对重要系统和数据库进行容灾备份，定期开展数据安全等级保护测试和渗透测试，关键设备应采用自主可控的产品和服务。

http://fgw.sz.gov.cn/zwgk/zcjzcjd/zc/content/post_10692431.html

8、《数据安全技术能力评估要求》等 3 项团体标准立项

7 月 4 日，中国互联网协会发布《数据安全技术能力评估要求》等 3 项团体标准立项的公告，《数据安全技术能力评

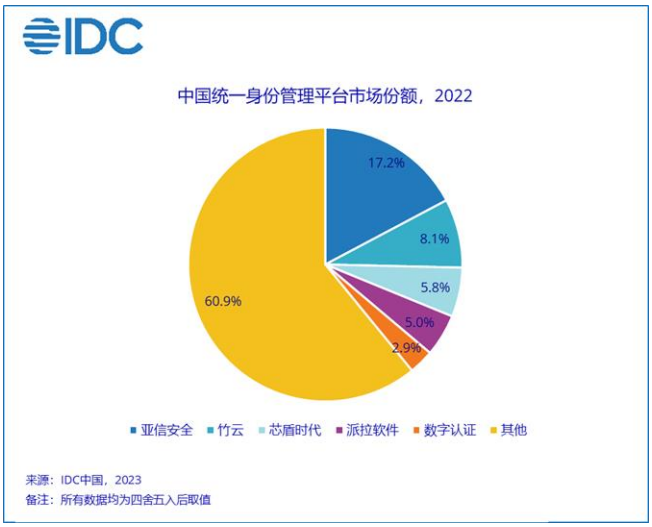
估要求》将规定应具备数据安全能力的企事业单位、政府部门等组织的数据安全技术能力要求，适用于第三方机构展开数据安全技术能力评估，为企业数据安全技术能力自评估提供参考和指导。

https://www.isc.org.cn/article/17166616918355968.html

技术、产品与市场

1、IDC：2022 年中国统一身份管理平台市场规模达 3.5 亿美元

IDC 于 2023 年 7 月正式发布了针对中国统一身份管理平台产品的市场份额研究报告，即:《中国统一身份管理平台市场份额，2022：安全建设，身份先行》(＃CHC50360223)。报告针对 2022 年中国统一身份管理平台市场的规模、增长速度、主要玩家、市场与技术的发展趋势等内容进行了详细研究。IDC 数据显示，中国统一身份管理平台市场在 2022 年实现了 7.1%的同比增长，规模达到 3.5 亿美元。由于身份安全在整体网络安全建设中处于十分关键的地位，市场中提供身份管理的厂商众多，而头部玩家仍然以在身份安全市场具备长期技术积累和市场培育的专业厂商为主，例如亚信安全、竹云、芯盾时代、派拉软件、数字认证等，具体情况详见下图:



https://www.secrss.com/articles/56272

2、IDC 发布《中国态势感知解决方案市场研究，2023》报告

态势感知平台的建设对于企业网络安全防御体系的重要程度越来越高，已经成为构建网络安全体系的核心，多年来持续受到客户的青睐。IDC 预测，到 2026 年，40%的拥有大量分支机构的大型企业组织将迁移到自动化安全运营中心（SOC）上，以加快其事件的修复、事件管理和响应速度。

从 IDC 调研来看，与过去两年相比，当前态势感知平台的核心能力提升包括但不限于:

（1）态势感知平台整体能力更趋向于实用化、实战化

（2）资产发现更精准

（3）威胁检测与响应效率更高效

（4）底层存储架构革新

（5）数据采集支持的探针接入种类丰富

（6）易用性持续提升

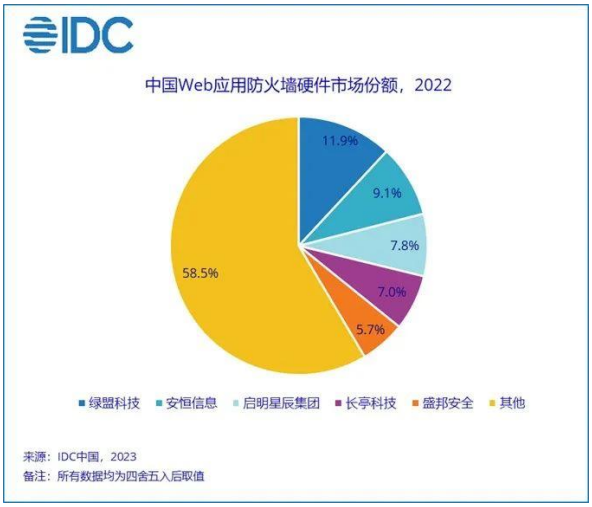
（7）公有云部署环境下态势感知平台云原生安全能力在持续加强

https://www.secrss.com/articles/56273

3、IDC：2022 年中国 WAF 市场规模为 2.06 亿美元

IDC 于 2023 年 6 月正式发布了针对中国硬件 WAF 和云 WAF 的两份市场份额研究报告，即：《中国 Web 应用防火墙硬件市场份额，2022：硬件增长受阻，寻求云上突破》（#CHC50361923）和《中国云 Web 应用防火墙市场份额，2022：云上云下协同发展，云原生 WAF 成为必然》（#CHC50357923）。报告针对 2022 年中国硬件 WAF、公有云 WAF 和私有云 WAF 市场的规模、增长速度、主要玩家、市场与技术的发展趋势等内容进行了详细研究。

IDC 数据显示，2022 年，中国硬件 WAF 市场呈现了-1.9%的同比增长，市场规模为 2.06 亿美元。具体情况详见下图：



https://www.secrss.com/articles/56150

4、云安全态势报告：95%的企业担心检测和响应能力

根据 Permiso 最新发布的云安全调查报告，云安全现状堪忧且存在重大认知误区。虽然 95%的企业担忧云安全检测和响应不足，但高达 80%的受访企业认为现有的工具和配置足以保护云环境的安全。

该调查评估了受访企业的云安全实践及其环境规模，包括企业用户管理的身份和机密信息的数量、对攻击的响应时间、访问其环境的不同方法以及使用的云安全解决方案类型。

报告的一些关键数据提供了云安全当前状态的整体视图：

- 50%的受访者报告称，由于未经授权访问其云环境而导致数据泄露。

- 95%的受访者担心他们当前的工具和团队可能无法检测和响应云环境中的安全事件。
- 55%的人将他们的担忧程度描述为“极其担忧”和“非常担忧”。
- 尽管很多企业存在高风险做法，并且普遍担心云环境中的漏洞，但超过 80%的受访者认为，他们现有的工具和配置足以保护他们的企业免受针对云环境的攻击。

https://www.secrss.com/articles/56144

5、原语科技发布专业 TEE 隐私保护计算解决方案「PrimiHub TEE」

原语科技推出了重量级项目「PrimiHub TEE」，它是基于 Intel SGX 技术的专业 TEE 隐私保护计算解决方案。PrimiHub TEE 分为远程认证和机密计算两大模块，使用 DCAP+PKI x509 证书链实现自建远程认证服务。该解决方案利用受信任的处理器和内存隔离技术，实现安全计算和隐私保护，提供高效的隐私保护计算能力。远程认证方案基于 DCAP+PKI x509 证书链，结合密钥协商协议，确保认证数据的完整性和真实性。计算流程包括任务提交、远程认证、密钥协商、数据加密和计算等环节，保证计算过程的安全性和

隐私性。

https://mp.weixin.qq.com/s/9FEyyNnPP70wibP9oY2Kaw

业界观点

1、方滨兴院士：模型加工场实现隐私保护与数据要素流通

7 月 6 日，BCS 2023 北京网络安全大会在北京国家会议中心开幕，中国工程院院士、中国电子信息产业集团首席科学家、鹏城实验室方向责任院士方滨兴发表了“模型加工场：一种支持隐私保护的数据使用权交易方法”的主题演讲。

他表示，**数据需要流通才能发挥最大价值，但隐私保护成为横亘在企业面前的大难题，模型加工场基于分享价值不分享数据的关键技术有望解决这一问题**。

方滨兴说，在数据流通中，数据提供方与消费方通过数据服务提供方进行交易，共同形成了数据要素流通交易市场。数据服务提供者要对数据提供安全技术保护，包括数据协商、访问控制、使用控制等。他指出，目前国际上已经有一些数据流通交易隐私保护实践。比如数据厂商 Snowflake 通过数据不动程序动，实现了数据提供方实时安全地共享数据获取数据收益。欧盟国际数据空间（IDS）基于数据所有权与使用权分离模式，已在多个行业开展实践探索，累计超过 50 个场

景案例。微软可信研究环境（TRE）使用安全输出机制，让研究人员在高安全控制和数据保护下访问和使用敏感数据。基于国际研究和工程实践，方滨兴提出兼顾隐私保护与数据要素流通的模型加工场技术。该技术包含五大要素：核心方法是数据不动程序动，关键技术是分享价值不分享数据，辅助手段是数据可用不可见，应用模式是保留所有权释放使用权，计算环境是算力网互联形成统一数据域。

https://mp.weixin.qq.com/s/tQxHx0d4HWfJ5EcfjcBzxg

2、倪光南院士：必须高度重视数据存储产业发展，加强顶层设计和战略布局

近日，信息化百人会学术委员、中国工程院院士倪光南在接受媒体专访时表示，数据存储产业将成为国家的战略性、基础性产业，成为新的国际竞争高地。我们必须高度重视中国数据存储产业发展，加强对此的顶层设计和战略布局，为掌握数字经济竞争主动权和科技强国建设提供坚实支撑。

对于问题“从全球先进存力的未来发展前景和行业趋势来看，我国先进存力应该如何发力”，倪光南院士表示，随着数字化转型的深入，新兴业务涌现，非结构化数据快速增长，进入 AI 大模型、自动驾驶训练等高价值生产场景；生成式 AI（AIGC）大模型带动数据爆发式增长，驱动数据存储基础

设施加快建设；数据安全威胁严峻，内生安全逐渐成为数据存储的必备能力。先进存力未来将迎来巨大的变革和发展机会。为了不失时机地推进中国数据存储产业的发展，他提出五点建议：

第一，产业发展，标准先行。为促进产业更好发展，可以行业标准或团体标准形式，发布“数据中心建设指南”，提出算力与存力适当比率范围；提出存力中采用 SSD 先进存力的适当比率范围，避免大力发展数据中心建设中的某些倾向，均衡部署和发展，抢占新一轮科技革命和产业变革制高点。

第二，政府在数据存储设备采购、招标中，可优先支持 SSD，不以单一价格指标作为评标依据；重要基础设施的数据存储设备，政府应政策引导，促进国产 SSD 产业发展。

第三，安全测评，公平公正。重视对数据存储产品的安全审查，包括供应链安全、信息安全、数据安全等等。尤其是对于数据存储整机、主控芯片、存储文件系统等等关键核心技术，建议实施自主可控测评，根据第三方测评机构给出的自主可控测评分值作为选择依据。

第四，重视高校数据存储产业人才培养。目前国内仅有 10+高校开展数据存储领域研究，领军教授 10+，博士队伍 100+，硕士不足 300 人。这与中国数据存储产业和应用市场体量不匹配。急需在高校增设数据存储专业、课程、实验室

等，扩大数据存储人才培养规模，并从收入、激励机制、基本公共服务等多角度构建新的人才政策，吸引并聚集国内外优秀人才。

第五，集聚产业，协同攻关。建议在国家科技攻关计划和相关产业链中设立数据存储专项，组织国内产学研用各界联合攻关，实现全产业链风险可控；成立数据存储国家实验室、国家级科创平台等，开展前沿技术研究，形成原创性成果，提升国产数据存储全球技术竞争力。

http://www.cbdio.com/BigData/2023-06/30/content_6174125.htm

3、陆志鹏：基于数据元件构建大模型数据底座推动数据要素流通

7 月 8 日，由上海数据交易所、大数据流通与交易技术国家工程实验室承办的“大模型时代下的数据要素流通”主题论坛在上海举行。中国电子党组成员、副总经理、中国电子数据产业有限公司党委书记、董事长陆志鹏围绕“数据要素驱动的大模型体系”做主旨演讲，他认为，大模型技术实现高质量发展，数据有效供给是关键，亟需建设安全可信的数据底座。当前数据合规确权、计量估价、协调分配、安全隐私保护等核心难题需要破解。

陆志鹏首先谈到大模型数据集的训练过程，他认为，大模型训练一般要经历以下流程：一般是公开数据，包括互联网数据、代码库，然后对这些数据进行半监管的训练，训练后形成了一个较为高质量的数据语料库以后，供大模型训练。

“但大模型公司可能会因为侵犯隐私和知识产权被起诉。”陆志鹏举例说，美国大模型出来后，就已经面临着一些法律风险。主要来自两个方面，一个是隐私，一个是知识产权。

大模型技术出现后，数据供应的过程中间遇到了什么问题？一是缺少合规确权的机制，目前国内面临的问题就是数据的有效供给不足。很多企业都在做语料库，但数据都非常有限，而且可能面临着统一标准的问题；二是缺少数据的计量估价机制；三是缺少协调分配；四是缺少安全隐私保护机制。

数据运算过程中，变量越多，大模型的反应就会越来越灵敏；参数越多，大模型的精准度越高，然而，面对大的参数计算机运算时，还要经过多层次的变化、多层次的降维才可以实现。如果数据量不经过加工治理，很难获得应用、很难挖掘价值，于是，利用“数据元件”，先把数据加工成元件，由元件来支撑流通、支撑模型训练。这样就有效地解决了四个问题。

https://mp.weixin.qq.com/s/e8awll0IfUcbUKGJTXfkKg

4、余晓晖：全球数字经济发展最新态势

2023 年 7 月 4-7 日，由北京市人民政府、工业和信息化部、商务部、国家互联网信息办公室、中国科学技术协会共同主办的“2023 全球数字经济大会”在北京召开。在 7 月 5 日上午的大会主论坛上，中国信息通信研究院院长余晓晖对全球数字经济发展最新态势进行了精彩解读。

主要国家数字经济发展持续提速。总体看，2022 年，美国、中国、德国、日本、韩国等 5 个世界主要国家的数字经济总量为 31 万亿美元，数字经济占 GDP 比重为 58%，较 2016 年提升约 11 个百分点；数字经济规模同比增长 7.6%，高于 GDP 增速 5.4 个百分点。产业数字化持续带动 5 个国家数字经济发展，占数字经济比重达到 86.4%，较 2016 年提升 2.1 个百分点。

具体来看，全球各国加快推动数字经济重点领域发展，在数字技术与产业、产业数字化、数据要素等领域积极抢抓发展机遇。

在产业数字化领域，全球产业数字化转型进入规模化扩张和深度应用阶段，数字化转型应用领域由生产研发向供应链协同、绿色低碳方向延伸，推动产业高端化、智能化、绿色化、融合化发展，助力提升产业链供应链韧性和安全。

在数据要素领域，近年来，各国将行业数据空间作为数据流通的关键基础设施，持续打造产业生态合力。主要经济体加快数据空间建设探索，欧盟在《数字欧洲计划》统一体系下，多主体协同推进公共/行业数据空间建设；美国依托云基础设施优势，面向数据流通进行产业转型升级；日本以点破面，通过指导现有基础设施向数据流通服务方向转型发展数据空间；中国加强行业数据空间应用牵引，开展行业龙头与初创企业产业生态培育。

https://mp.weixin.qq.com/s/Us7ec4e7-e8S4BWwgfOWHA

5、从“毕业生盗取学生信息”事件，看高校数据安全的六个问题、三个关键

近日，中国人民大学毕业生马某，在读硕士研究生期间通过非法技术手段，盗取了近几届学生的个人信息，并制作成网页供任何人随意浏览，甚至能够给该校女学生的颜值打分。目前，中国人民大学已第一时间联系警方，该毕业生被依法刑事拘留，案件正在进一步调查中。

整体来看，高校数据安全能力还在起步阶段，伴随数字化的深入开展，威胁手段的持续升级，新问题、新风险交织，高校数据安全这六个问题需要重点关注：

（1）数字化转型造成数据敏感级别不断提升；

（2）数据安全管理制度体系不够完善 ；

（3）工作人员缺乏数据安全意识;

（4）数据安全精细化管控措施普遍缺位;

（5）系统运维特权账号缺少管控措施;

（6）API 数据共享安全风险难感知。

针对高校数据安全现状和主要问题，应以数据分类分级为起点，以管理制度为依据，在具体建设过程和环节中，充分利用和发挥好各种关键技术的作用，分段实施，体系规划，逐步构建覆盖数据全流程、全链路的数据安全防护技术体系，最后构建数据安全运营体系，实现数据安全的持续优化和提升:

（1）分类分级是建设基础。经过多年信息化建设，高校已积累了规模庞大的数据资产，且涉及的信息量及群体规模十分复杂，数据资产有哪些？怎么分布？有哪些类型？借助技术手段摸清资产家底，进行数据分类分级成为数据安全建设的首要任务。

（2）管理制度是建设依据。《教育部等七部门关于加强教育系统数据安全的通知》中明确，应健全覆盖数据收集、传输存储、使用处理、开放共享等全生命周期的数据安全保障制度。对此，高校在制定数据安全管理与隐私保护相关办法中，需明确数据收集、存储、处理、共享等关键环节的操

作规范、管理部门职责分工、应急管理与安全检查机制，充分发挥各部门和各类人员在数据安全保障工作中的作用，共同遵守和执行安全规章制度，保障数据安全策略的贯彻落实。

（3）数据安全需全链路建设。数据在流动中创造价值，对数据的保护就是对流动过程的数据全链路分级保护。在数据安全建设中，高校需梳理数据应用重要业务场景，评估其数据安全现状，在数据分类分级的基础上，分段实施、体系规划、面向数据访问域、存储域、流动域，落实覆盖数据全链路的数据安全技术防护体系。

https://www.donews.com/news/detail/4/3581540.html

数据安全事件

1、罚款 5 万元！中山警方开出该市首张违反《数据安全法》罚单

近日，中山三乡公安分局鹤湾派出所在对辖区内的公司进行数据安全检查过程中，**发现一家信息科技公司疑似存在网络数据泄露隐患**。鹤湾派出所通过询问相关责任人、调取网络设备日志信息、开展技术检测等方式，**发现该公司在没有依法建立数据安全管理制度和操作规程等数据保护措施的前提下，对存储的公民敏感信息数据未采取去标识化和加密保护**。通过现场检查，发现该公司用于存储公民敏感信息的服务器**也存在未授权访问的漏洞，用户隐私数据存在泄露风险。**根据《中华人民共和国数据安全法》第二十七条、第四十五条之规定，三乡公安分局对该公司未履行数据安全保护义务的违法行为，依法对该公司处以警告以及罚款 5 万元的行政处罚，对该公司负责人作出罚款 1 万元的行政处罚。该公司负责人表示接受处罚，并将严格按照公安机关要求整改，切实履行网络安全主体责任。

https://www.secrss.com/articles/56232

2、两家使用 Google Analytics 的公司被瑞典罚款 110 万美元

据 7 月 4 日报道，瑞典隐私保护局(IMY)对两家使用 Google Analytics 的公司罚款 1230 万瑞典克朗（约合 110 万美元），并警告另外两家公司不要采取同样的做法。具体来说，这些公司违反了 GDPR 第 46(1)条，该条禁止将个人数据传输到缺乏安全保障和法律补救机制的国家或国际组织。IMY 认为通过 Google Analytics 工具传输到美国的数据是个人数据，还得出结论，这些公司采取的技术安全措施不足以确保基本上符合欧盟所保障的保护水平。Meta 曾因该问题被 DPC 罚款 13 亿美元。

https://www.bleepingcomputer.com/news/security/google-analytics-data-transfer-to-us-brings-1-million-fine-to-swedish-firms/

3、台积电遭遇天价数据勒索：硬件供应商被黑，泄露少数内部数据

7 月 3 日消息，全球最大芯片代工企业台积电在上周五表示，由于硬件供应商 Kinmax Technology 发生一起“安全事件”，攻击者获取了台积电企业网络中一些服务器的配置和设置信息。

此消息公布前一天，LockBit 勒索软件犯罪团伙在其敲

诈网站上“点名”台积电，并威胁道：如不支付 7000 万美元赎金，将公开所窃数据。

Kinmax 公司证实，测试环境遭到外部团体的攻击，攻击者成功检索了配置文件和其他参数信息。该公司还表示，于 6 月 29 日得知此次入侵，立即关闭了受损系统并通知了受影响客户。台积电代表在一封电子邮件中写道：“经过审查，此事件没有影响到台积电的业务运营，也没有泄露任何台积电的客户信息。事件发生后，台积电根据公司安全规程和标准操作程序立即终止了与该供应商的数据交换。”声明没有提及攻击者是否已经联系台积电，或是台积电是否准备支付赎金。

https://www.secrss.com/articles/56232

4、知名律所遭勒索软件攻击，澳大利亚政府军队等客户数据泄露

澳大利亚律所 HWL Ebsworth 遭勒索软件窃取 4TB 敏感数据：军队、政府、银行等核心客户受影响。

该律师事务所的一份数据泄露通知证实，该律师事务所于 4 月 28 日发现暗网帖子夸耀被盗信息，并且其部分机密客户信息于 6 月 9 日被 ALPHV/BlackCat 泄露。

HWL Ebsworth 还披露了其内部公司数据的严重泄露，包括信用卡号、贷款信息、员工简历和访问凭证。位于墨尔

本的服务器总共约有 4 TB 的数据被盗。据报道，ALPHV/BlackCat 索要 500 万澳元的赎金，但 HWL Ebsworth 迄今拒绝支付，导致攻击者部分数据泄露。

https://www.secrss.com/articles/56136

5、日本最大的港口名古屋港遭勒索软件攻击，造成巨大经济影响

近日日本名古屋港口遭遇了一次勒索软件攻击，影响了集装箱码头的运作。名古屋港口运输协会也已经证实，此次网络攻击扰乱了集装箱进出港口的工作。

据名古屋港口管理协会透露，7 月 4 日上午 6 时 30 分左右，日本网站 FNN 报道称该港口得到集装箱码头发生了系统故障。除了在拖车上装卸集装箱外，装卸工作已经停止。

名古屋港当局与负责运营该系统的名古屋港口运营协会码头委员会以及爱知县警察总部举行了会议，发现问题是由勒索软件攻击导致的。这次安全事件将对港口造成巨大的经济影响。专家预估，此次攻击事件还可能影响全国各地的货物运输。

https://hackernews.cc/archives/44441

6、西门子能源遭遇勒索软件攻击，大量数据被盗

近日，西门子能源称其遭遇了一次 Clop 勒索软件攻击，该软件利用 MOVEit Transfer 平台的一个零日漏洞窃取了公司数据。

6 月 27 日，Clop 在其数据泄露网站上列出了西门子能源公司，并表示盗取了该公司的数据。西门子能源公司的一位发言人证实 Clop 勒索软件利用 CVE-2023-34362 的 MOVEit 传输零日漏洞入侵了西门子。不过西门子能源公司表示，目前暂时还没有关键的数据被盗，业务运营也没有受到影响，他们在得知这一事件后也立即采取了行动。

https://hackernews.cc/archives/44320

7、孟加拉国政府网站泄露数百万公民数据

7 月 7 日消息，一名研究人员最近发现孟加拉国政府网站泄露了数百万公民的个人数据。据最先报道该消息的 TechCrunch 报道，泄露的数据包括全名、电话号码、电子邮件地址和身份证号码。

https://securityaffairs.com/148264/data-breach/bangladesh-government-website-data-leak.html

8、美国儿童电视频道 Nickelodeon 约 500 GB 数据泄露

媒体 7 月 6 日称，有传言称尼克儿童频道(Nickelodeon)动画部门发生了重大的泄密事件。所谓数据泄露的证据开始在社交媒体上流传，显示为大量文档和媒体文件，据称大小高达 500 GB。Nickelodeon 公司已经证实，这些涉嫌违规泄露的数据是合法的，但其中的一些似乎是几十年前的。据推测，数据泄露事件发生在今年 1 月。Nickelodeon 发言人表示，调查正在进行中，分析可能需要一段时间，但似乎没有发现真正入侵的迹象。

https://www.theregister.com/2023/07/06/nickelodeon_confirms_data_leak/

9、瑞士两家出版社遭到 Play 的攻击，泄露约 42 万人的信息

据媒体 7 月 4 日报道，《瑞士评论》订阅者的信息在暗网被公开，包含超过 425000 个地址，其中 40%是邮政地址，60%是电子邮件地址。所有在瑞士注册为海外公民的人都会自动通过电子邮件或邮寄的方式收到《瑞士评论》。瑞士政府认为泄露的数据非常敏感，甚至连《瑞士评论》的出版商 SwissCommunity 都无法访问这些数据。据悉，此次泄露源于 Play 对两家瑞士出版社（NZZ 和 CH Media）的勒索攻击导致的。这些公司表示，他们尚未交赎金。

https://www.swissinfo.ch/eng/politics/data-leak-affects-425-000-swiss-abroad/48628744

10、美国医疗保健公司违规，儿童患者数据面临风险

7 月 4 日消息，ARx 医疗保健公司表示，他们在 2022 年遭受了一次网络攻击，可能暴露了 4 万多名患者的个人资料，其中许多是儿童患者。目前还不清楚为什么直到现在才披露这个消息。

据总检察长称，只有 526 名缅因州居民受到影响，但潜在受害者总数达到 41,166 人，目前尚不清楚这些人是否都是患者，或者该数字是否还包括可能已被感染的第三方承包商的详细信息。保留在 ARx 的内部系统上。似乎可以肯定的是，这家医疗保健公司去年 3 月遭受了一次系统入侵，泄露了包括儿童患者姓名、处方信息、保险和账号、医生姓名以及（在某些情况下）社会安全号码在内的详细信息。

https://cybernews.com/privacy/us-healthcare-breach-child-patient-data/

11、美国专利局数据泄露暴露商标申请

6 月 30 日，美国专利商标局 (USPTO) 通知超过 60,000 名商标申请提交者，其错误地将他们的物理地址暴露在公共

互联网上三年。

据报道，泄漏的 API 是罪魁祸首，它导致数据集暴露，包括从申请人那里收集的地址，这些地址在向美国专利商标局 (USPTO) 申请商标时是强制性的。此次泄露影响了三年期间提交的约 3% 的申请。

https://www.darkreading.com/physical-security/us-patent-office-hacked-trademark-apps-accessed

12、英国 NHS 超过 100 万名患者的详细信息因网络攻击泄露

据 6 月 29 日报道，英国 NHS 超过 100 万患者的详细信息已在网络攻击中泄露。据悉，曼彻斯特大学近期遭到勒索攻击，影响了 NHS 患者数据库，涉及 200 家医院 110 万名患者的信息，这些信息是由该大学出于研究目的而收集的。根据该大学进行的一项调查，分析表明大约 250 GB 的数据被访问。曼彻斯特大学发言人拒绝就 NHS 数据发表评论，但没有否认这一数据泄露事件。

https://www.independent.co.uk/news/health/nhs-patient-data-attack-b2364202.html

《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