

全球数据安全观察

总第 73 期 2022 年第 01 期
(2021.12.27-2022.01.02)

目录

政策形势	1
1、中央网信办发布《“十四五”国家信息化规划》	1
2、福建省人大通过《福建省大数据发展条例》	1
3、交通运输部印发《数字交通“十四五”发展规划》	2
4、《网络安全标准实践指南——网络数据分类分级指引》全文发布.....	3
5、国家互联网信息办公室等十三部门修订发布《网络安全审查办法》	4
业界观点	5
1、周鸿祎：元宇宙安全本质是数字安全 将迎来数字文明时代.....	5
2、安全未来 2021：数字安全能力成刚需	6
3、中国信通院发布《数据安全技术与产业发展研究报告（2021年）》	6
4、企业数据丢失防护 (DLP) 市场年复合增长高达 21% ...	8
5、隐私计算如何规模化应用——基于隐私计算一体机的解决方案.....	9
安全事件	10
1、物流巨头 DW Morgan 暴露了 100 GB 的客户数据	10
2、惠普超算备份错误导致京都大学损失 77TB 研究数据..	10
3、全球最大图片服务公司 Shutterfly 遭 Conti 勒索软件攻击	11
4、越南公司 ONUS 遭勒索攻击，拒绝支付 500 万美元赎金	11
5、T-Mobile 遭遇新的数据泄露	12
6、美医疗系统 Broward Health 披露数据泄露事件 影响超 130 万人.....	12

政策形势

1、中央网信办发布《“十四五”国家信息化规划》

12月27日，中央网络安全和信息化委员会印发《“十四五”国家信息化规划》，围绕确定的发展目标，部署了10项重大任务。《规划》围绕确定的发展目标，部署了10项重大任务，一是建设泛在智联的数字基础设施体系，二是建立高效利用的数据要素资源体系，三是构建释放数字生产力的创新发展体系，四是培育先进安全的数字产业体系，五是构建产业数字化转型发展体系，六是构筑共建共治共享的数字社会治理体系，七是打造协同高效的数字政府服务体系，八是构建普惠便捷的数字民生保障体系，九是拓展互利共赢的数字领域国际合作体系，十是建立健全规范有序的数字化发展治理体系，并明确了5G创新应用工程等17项重点工程作为落实任务的重要抓手。

<https://www.freebuf.com/news/317579.html>

2、福建省人大通过《福建省大数据发展条例》

福建省十三届人大常委会第三十次会议表决通过《福建省大数据发展条例》，将于明年2月1日起施行。《条例》从数据资源、基础设施、发展应用、数据安全、保障措施和

法律责任等方面对大数据的发展作出了具体规定。

在数据采集方面，《条例》规定采集数据应当向被采集者公开采集规则，明示采集目的、方式和范围，并经被采集者同意。凡能通过共享获取的公共数据，政务部门不得重复采集。同时，为解决部门间数据壁垒、共享不充分等问题，《条例》明确公共数据以共享为原则、不共享为例外，分为无条件共享、有条件共享和暂不共享3种类型。凡列入暂不共享类公共数据的，应当有法律、行政法规或者国家政策作为依据。

在公共数据开放方面，《条例》明确应当优先开放与民生密切相关、社会关注度和需求度高的数据。公开数据分为普通开放和依申请开放两种类型。

在数据开发利用方面，《条例》规定，依法获取的各类数据经处理无法识别被采集者且不能复原的，可以交易、交换或者以其他方式开发利用。按照有关规定开发利用公共数据资源获得的合法收益，受法律保护。

https://baijiahao.baidu.com/s?id=1719349892116219375&wfr=s_pider&for=pc

3、交通运输部印发《数字交通“十四五”发展规划》

为科学推动“十四五”时期数字交通发展，近日，交通运

输部印发《数字交通“十四五”发展规划》，以数字化、网络化、智能化为主线，以改革创新为根本动力，以先进信息技术赋能交通运输发展，强化交通数字治理，统筹布局交通新基建，推动运输服务智能化，培育产业创新发展生态，加强网络安全保障体系和能力建设，有效提升精准感知、精确分析、精细管理、精心服务能力，促进综合交通高质量发展，为加快建设交通强国提供有力支撑。

其中要求，**打造综合交通运输“数据大脑”**。完善部、省两级综合交通运输信息平台架构，推进综合交通大数据中心体系建设，加强数据资源的整合共享、综合开发和智能应用。

<https://mp.weixin.qq.com/s/mK5qcHOrKaEn-toItfiWUQ>

4、《网络安全标准实践指南——网络数据分类分级指引》全文发布

2021年12月31日，全国信息安全标准化技术委员会秘书处发布了《网络安全标准实践指南——网络数据分类分级指引》，给出了网络数据分类分级的原则、框架和方法。

数据分类分级框架中，《实践指南》提出：常见的数据分类维度包括**公民个人维度、公共管理维度、信息传播维度、组织经营维度、行业领域维度**；从国家数据安全角度可将数

据分为一般数据、重要数据、核心数据共三个级别；建议数据处理器优先按照基本框架进行定级，在基本框架定级的基础上也可结合行业数据分类分级规则或组织生产经营需求，对一般数据进行细化分级。

<https://mp.weixin.qq.com/s/vaogX-6LBSfKSemKlqgJJQ>

5、国家互联网信息办公室等十三部门修订发布《网络安全审查办法》

近日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局等十三部门联合修订发布《网络安全审查办法》（以下简称《办法》），自2022年2月15日起施行。

《办法》将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查，并明确掌握超过100万用户个人信息的网络平台运营者赴国外上市必须向网络安全审查办公室申报网络安全审查。根据审查实际需要，增加证监会作为网络安全审查工作机制成员单位，同时完善了国家安全风险评估因素等内容。《办法》修订对保障国家网络安全和数据安全具有重要意义。

https://mp.weixin.qq.com/s/o-4Us_Xys0bXt8-CZJDD6w

业界观点

1、周鸿祎：元宇宙安全本质是数字安全 将迎来数字文明时代

数字化程度越高，安全挑战越大，未来对虚拟世界的攻击会伤害到现实世界，因此元宇宙面临的安全风险，本质也是数字安全带来的挑战。国家层面提出统筹传统安全与非传统安全，提升网络安全、数据安全、人工智能安全等领域的治理能力，标志着数字安全元年开启，进入到大安全时代。

“就像一千个人眼中，就有一千个哈姆雷特一样，一千个人眼中，就有一千个元宇宙。”周鸿祎认为，元宇宙仍是一个不断发展、演变的概念，很难说有定论，但需要注意的是，元宇宙为大家提供充分想象空间的同时，也引来游戏派、炒股派、炒币派、社区派等各种流派炒作，透支着行业的未来。

但归根结底，周鸿祎认为元宇宙是构建在人工智能、大数据、云计算、区块链、等数字化技术逐渐成熟、融合推动的基础之上，是数字化发展到高级阶段的产物。他赞成产业元宇宙，通过构建和真实世界完全打通的虚拟空间，为真实世界提供更好的数字化支持。

<https://mp.weixin.qq.com/s/6B9NcmTDvbFRSn5uwcl9sw>

2、安全未来 2021：数字安全能力成刚需

2021年12月30日，三六零(601360.SH, 下称“360”)未来安全研究院在年度思想荟上重磅推出“数字安全观察知识情报平台”，并举行平台首发仪式。据介绍，该平台定位是安全战略研究和前沿认知体系(DSI)，旨在建立战略研究生态，洞察数字化时代的网络空间安全发展趋势，帮助决策者看清未来并作出正确决策。

“数字时代，安全挑战正急速扩张到更多新领域，并发生质变升级为数字安全。”数字安全不仅仅是企业的成本，而是会成为企业的刚需与竞争力。目前，数字安全需要从以产品为中心转向以能力为中心，已经成为行业共识。“只有形成安全能力，并以实战作为最终目标，才能应对数字安全挑战，而且安全能力需要可衡量，可持续成长。”大量和安全相关的标准开始聚焦能力或者能力成熟度，数字安全已经迈进能力主义时代。

https://mp.weixin.qq.com/s/u_8ta1JfOFYiABxlwHg-Qg

3、中国信通院发布《数据安全技术与产业发展研究报告(2021年)》

近日，中国信通院安全研究所研究编制了《数据安全技术与产业发展研究报告(2021年)》。报告通过调研访谈的

方式研究梳理我国数据安全技术、产品和服务的发展驱动力以及现状，形成总体的数据安全技术与产业发展视图。

报告显示：**一、数据安全产品体系逐步完善，总体处于快速发展期。**国内数据安全产品已经从单一的数据库加密、审计扩展到数据资产管理、安全防护、监测/检测、共享流通安全、隐私保护、追踪溯源等数据全生命周期的方方面面。

(1) 数据资产管理、数据分类分级产品市场需求明显，但产品名称五花八门，产品功能各异，产品性能不尽如人意；(2) 数据库加密、数据库防护、数据库审计、动/静态数据脱敏，数据防泄漏等安全产品也进入成熟期，各家产品的功能基本相似，应用场景明确，应用行业广泛；(3) 数据水印、数据溯源等产品处于萌芽期，仅有 15%的企业推出了相关产品；

(4) 隐私计算产品商用化处于起步阶段，主要集中于金融行业的智能风控、智能营销、反洗钱等少数几个场景，其他行业应用较少，因为使用隐私计算成本过高，且企业对数据共享的监督能力较弱，隐私计算产品尚未得到广泛应用。

二、数据安全服务占比相对较低，总体趋势向好。目前国内市场上的数据安全服务主要涵盖数据安全合规评估、数据安全规划咨询、数据安全治理(分类分级)三大类，数据安全托管、数据安全运维、数据安全测评、数据安全防护能力评定等服务开展较少。

<https://www.wangan.com/p/7fy7fgedcf65919a>

4、企业数据丢失防护 (DLP) 市场年复合增长高达 21%

根据 ResearchAndMarkets 最新发布的调查数据，未来五年全球企业数据丢失防护 (DLP) 市场预计将以 21.03% 的复合年增长率高速增长，到 2026 年市场规模将达到 62.65 亿美元，而 2019 年为 16.47 亿美元。

DLP 解决方案可按照网络、存储/数据中心、端点、服务、咨询、系统集成、培训等不同应用领域进行分类。根据部署模式，DLP 还可分为内部部署和云端防护两大类。由于云数据丢失防护为电子邮件、USB 驱动程序、笔记本电脑和移动电话提供了解决方案，因此预计云 DLP 细分市场将会进一步增长。

从垂直行业来看，新兴行业中越来越多地开始使用企业数据丢失防护，此外，航空航天和国防、通信和技术、政府、医疗、制造和其他行业的 DLP 市场也将以高复合年增长率增长。

<https://www.secrss.com/articles/37741>

5、隐私计算如何规模化应用—基于隐私计算一体机的解决方案

隐私计算一体机是在云原生环境下打造的集软硬件安全可信于一体的平台系统，秉持安全与可信并重的原则，提供数据安全和隐私保护的可信数据计算平台。

隐私计算一体机整体分为 IaaS 层和 PaaS 层，在 IaaS 层可信根作为隐私计算一体机可信的源头，支持可信平台实现可信链传递，GPU 和 FPGA 实现算法加速能力，有效提升隐私计算算法性能。PaaS 层基于 IaaS 层的基础能力，提供远程认证服务、密码服务、隐私计算服务和算法加速服务等。

<https://mp.weixin.qq.com/s/sEsxqopp79UiZw9v6vItQw>

安全事件

1、物流巨头 DW Morgan 暴露了 100 GB 的客户数据

2021 年 12 月 28 日，Website Planet 安全团队发现了跨国物流巨头 DW Morgan 遭受的数据泄露。该数据泄露由开放的 AWS S3 存储桶暴露引起，据研究人员称，这些数据与运输和公司客户有关，其中包括思科和爱立信等财富 500 强公司。该数据库包含价值超过 100 GB 的数据和 250 万个文件，详细说明了属于 DW Morgan 全球员工和客户的财务、运输、运输、个人和敏感记录。

<https://securityaffairs.co/wordpress/126086/data-breach/d-w-morgan-data-leak.html>

2、惠普超算备份错误导致京都大学损失 77TB 研究数据

2021 年 12 月 30 日，据报道，由于惠普公司超级计算机的备份系统出现错误，导致日本京都大学约 77TB 的科研数据被误删。该事件发生在 2021 年 12 月 14 日至 16 日，14 个科研小组的 3400 万份文件从系统和备份文件中被删除。据悉，备份程序本应使用 `find` 命令删除超过 10 天的旧日志，但其错误地执行了包含未定义变量的 `find` 命令，删除了

/LARGE0 目录下的正常文件。目前，该大学已废弃该备份系统，并计划在 2022 年 1 月重新引入。

<https://www.bleepingcomputer.com/news/security/new-flagpro-malware-linked-to-chinese-state-backed-hackers/>

3、全球最大图片服务公司 Shutterfly 遭 Conti 勒索软件攻击

2021 年 12 月 28 日报道，摄影和个性化照片巨头 Shutterfly 近日遭到 Conti 的勒索软件攻击，据称该软件已经加密了 4000 多台设备和 120 台 VMware ESXi 服务器，并窃取了企业数据，勒索软件团伙要求数百万美元的赎金。

Conti 创建了一个私人的 Shutterfly 数据泄漏页面，其中包含据称在勒索软件攻击中被盗的文件截图，作为这种“双重敲诈”战术的一部分。攻击者威胁说，如果不支付赎金，将公开这个页面。

https://mp.weixin.qq.com/s/z2HLbi_dtavwjOpAB9CarA

4、越南公司 ONUS 遭勒索攻击，拒绝支付 500 万美元赎金

2021 年 12 月 29 日报道，越南的金融科技公司 ONUS 遭到勒索攻击。12 月 11 日至 13 日期间，攻击者成功利用 ONUS Cyclos 服务器上的 Log4Shell 漏洞，并植入后门。Cyclos 在

13 日发布公告称修复其系统，但此时为时已晚。攻击者已窃取该公司近 200 万条客户记录，包括 E-KYC 数据、个人信息和密码。12 月 25 日，ONUS 拒绝支付 500 万美元的赎金之后，攻击者开始出售窃取的数据。

<https://www.bleepingcomputer.com/news/security/fintech-firm-hit-by-log4j-hack-refuses-to-pay-5-million-ransom/>

5、T-Mobile 遭遇新的数据泄露

2021 年 12 月 29 日报道，T-Mobile 披露了一项新的数据泄露事件，该事件影响了作为 SIM 交换攻击受害者的“极少数客户”。根据查看 T-Mobile 内部文件的 *T-Mo 报告*，某些客户帐户存在“未经授权的活动”。攻击者查看客户专有网络信息（CPNI），并对少数客户进行 SIM 交换攻击。

<https://securityaffairs.co/wordpress/126140/cyber-crime/t-mobile-suffered-data-breach.html>

6、美医疗系统 Broward Health 披露数据泄露事件 影响超 130 万人

2022 年 1 月 4 日报道，美国 Broward Health 公共卫生系统近日披露了一起大规模数据泄露事件，影响到 1357879 人。Broward Health 是一个位于佛罗里达州的医疗系统，有三十

多个地点提供广泛的医疗服务，每年接收超过 60000 名入院病人。调查显示，一名入侵者未经授权访问了医院的网络和病人数据，其中可能包括病人的全名、出生日期、地址、电话号码、财务或银行信息、医疗诊断等等。

<https://www.cnbeta.com/articles/tech/1221691.htm>