全球数据安全观察

总第 102 期 2022 年第 30 期

(2022.08.15-2022.08.21)

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
1、中央网信办：正在加快推动《未成年人网络保护条例》出台.....1
2、未落实通信网络安全防护管理责任，上海 6 家单位被通报.....1
3、全国信安标委对《网络安全标准实践指南——健康码防伪技术指南（征求意见稿）》征求意见.....2
4、郑州数据交易中心揭牌运营.....2
5、美国联邦贸易委员会征求公众意见：拟规制商业监控及数据安全.....3
6、俄罗斯修订《联邦个人数据法》，强化运营商数据安全责任.....4
技术、产品与市场.....5
1、Gartner 发布 2022 年新兴技术成熟度曲线，25 项新兴技术中隐私计算占 6 项.....5
2、《数字政府行业趋势洞察报告（2022 年）》：预计 2023 年政务云市场规模将达到 1203.9 亿元.....7
3、2021 年中国隐私计算市场规模.....8
4、单核 CPU 破解后量子加密候选算法只需一小时.....10
5、2022 年上半年报告了近 2,000 起数据泄露事件.....11
业界观点.....13
1、冯登国院士：关键信息基础设施安全保护三大关键能力.....13
2、邬贺铨：从实践中深化对数据中心“数学”与“算术”的认识.....14
3、李苏：基层央行视角下的金融数据安全管理探索.....15

4、杨殿阁：数据安全管理关乎智能汽车竞争胜负 16
5、穆飞：数字化转型过程工作重点及挑战调研 17
数据安全事件 19
1、印度金融服务公司 37,000 名用户的个人数据、交易详情在线泄露.....19
2、微软员工在 GitHub 上意外泄露内部敏感登录凭据.....19
3、攻击 Twilio 的黑客暴露了 1900 名用户的 Signal 电话号码.....20
4、超 9,000 台 VNC 服务器在没有密码的情况下在线暴露.....21
5、航空航天和国防巨头遭受网络攻击，大量数据被窃取.21
6、CS:GO 最大交易平台遭黑客攻击，600 万美元游戏皮肤失窃.....22
7、黑客利用 0-day 漏洞从比特币 ATM 中窃取加密货币.23
8、英国一水厂疑遭勒索软件攻击，IT 系统中断服务敏感数据或泄露.....23
9、英特尔新型 CPU 漏洞可致敏感数据泄露 24
10、阿根廷科尔多瓦司法机构遭到 Play 团伙的勒索攻击..24

政策形势

1、中央网信办：正在加快推动《未成年人网络保护条例》出台

8 月 18 日，中共中央宣传部举行“中国这十年”系列主题新闻发布会，中央网信办副主任、国家网信办副主任盛荣华在会上介绍，当前，中央网信办正在加快推动《未成年人网络保护条例》出台，完善《未成年人保护法》的配套制度，为未成年人网络保护提供更加有力的法律保障。

银保监会披露的银行保险机构侵害个人信息权益乱象主要包括个人信息收集、个人信息存储和传输、个人信息查询、个人信息使用、个人信息提供、个人信息删除以及第三方合作等 7 类，本次专项整治工作将通过自查整改、监管抽查、总结汇报三个阶段推动落实。

https://mp.weixin.qq.com/s/2XiUtL6Oo3twTt2P9Jivrg

2、未落实通信网络安全防护管理责任，上海 6 家单位被通报

8 月 15 日晚，上海市通信管理局发布了关于通信网络安全防护管理情况的通报（2022 年 7 月）。

根据《网络安全法》《通信网络安全防护管理办法》《公

共互联网网络安全威胁监测与处置办法》等法律法规和《上海市通信管理局关于加强电信和互联网行业通信网络安全防护管理工作的通知》要求，上海市通信管理局定期对本市电信和互联网企业的通信网络安全防护管理情况进行督查审查，并对在本市行政区域内提供通信网络安全评测、评估服务的网络安全专业机构及其信息通信领域安全服务资质予以备案登记。

上海市通信管理局检查发现，6 家单位存在未落实通信网络安全防护管理责任等违规行为。

https://www.anquanke.com/post/id/278059

3、全国信安标委对《网络安全标准实践指南——健康码防伪技术指南（征求意见稿）》征求意见

8 月 16 日，为指导健康码技术提供方提升健康码技术防伪能力，全国信息安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南——健康码防伪技术指南（征求意见稿）》，并面向社会公开征求意见。

https://mp.weixin.qq.com/s/qSMD23wGbczi0ih3OYavIg

4、郑州数据交易中心揭牌运营

8 月 21 日，郑州数据交易中心揭牌仪式启动。郑州数据

交易中心由河南省工业和信息化厅推动组建，旨在充分发挥数据交易中心在数据要素市场中枢纽作用，本着打造更加完善的数据要素流通生态的理念，引导数据要素交易生态加速汇集，形成基础夯实、布局合理、特色鲜明、协同高效数据交易生态圈。

据了解，郑州数据交易中心采用公司制架构，围绕建设国内领先的数据要素流通服务平台目标，通过交易系统、场景驱动、监管体系、产业生态四个方面的创新，提供安全、可信、高效的交易环境，促进数据要素可信流通和开发利用，释放数据价值，推动河南省数据经济高质量发展。

https://mp.weixin.qq.com/s/uLLvm8YgcufVZ_lgSpXzQw

5、美国联邦贸易委员会征求公众意见：拟规制商业监控及数据安全

美国联邦贸易委员会（FTC）近日向社会公开征集意见，该机构正在探索打击有害的商业监控和松懈的数据安全规则，这将是美国联邦政府为科技行业制定隐私监管制度迈出的第一步。

《关于拟议中制度制定的预先通知》（Advance Notice of Proposed Rulemaking ）就商业监控造成的危害以及是否需要新规则来保护人们的隐私和信息征求公众意见。FTC 认为，

商业监控是一项收集、分析和利用个人信息的业务。大规模监控增加了数据泄露、欺骗、操纵和其他滥用的风险。

https://www.ipeconomy.cn/index.php/index/news/magazine_details/id/5631.html

6、俄罗斯修订《联邦个人数据法》，强化运营商数据安全责任

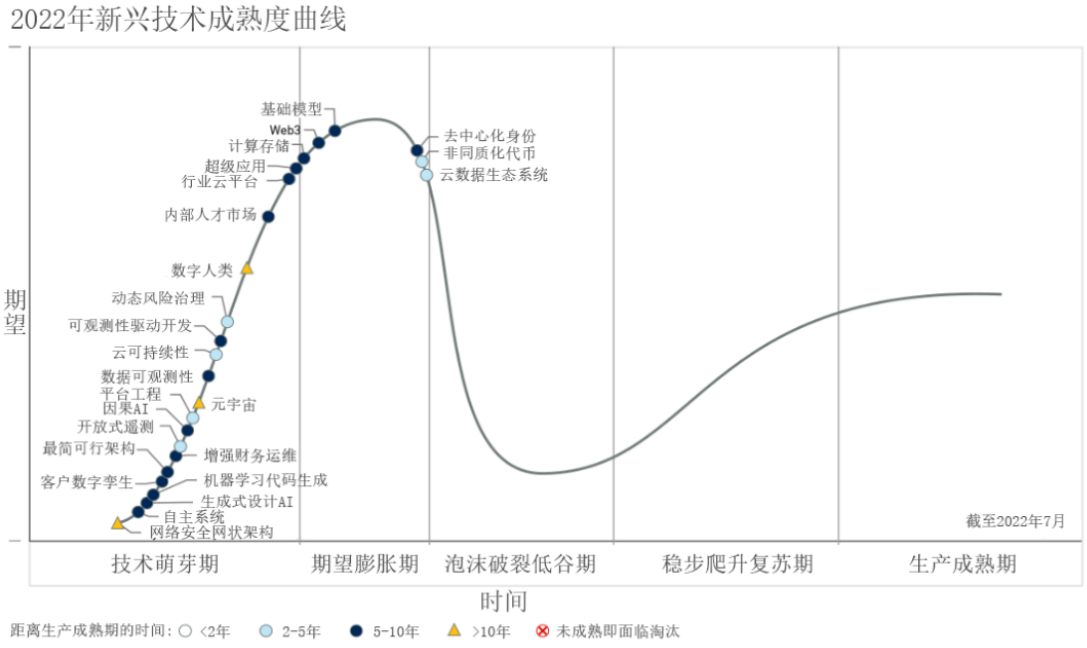
8 月 11 日，，俄罗斯联邦通信、信息技术和大众传媒监督局（Roskomnadzor）领导的公共委员会举行了例行会议，会上讨论了最近通过的《联邦个人数据法》的变化以及在数字服务发展的背景下保护其主体的权利。据专家介绍，将加强对用户的保护以及数据运营商的泄密责任。部分修正案将于将于 9 月 1 日生效。

https://www.secrss.com/articles/45900

技术、产品与市场

1、Gartner 发布 2022 年新兴技术成熟度曲线，25 项新兴技术中隐私计算占 6 项

Gartner 2022 年新兴技术成熟度曲线列出了 25 项值得关注的新兴技术，这些技术正在推动沉浸式体验的发展和扩展、加速人工智能（AI）自动化并优化技术人员交付。**新兴技术趋势的三个主题：沉浸式体验不断发展和扩展、AI 自动化提速、技术人员交付得到优化。**



今年的前沿热门技术共 25 项，其中隐私计算相关技术高达 6 项，占比 24%，绝对称得上当前兼具潜力价值和讨论热度的前沿技术领域。25 项新兴技术中与隐私计算相关的有：**去中心化身份、元宇宙、非同质化代币、Web3、网络安全网**

格架构、数据可观察性。

去中心化身份：允许实体（通常是用户）利用区块链或其他分布式账本技术以及数字钱包来控制自己的数字身份。去中心化身份的过程涉及到身份匿名、加密存储等，这些都是隐私计算的基础技术架构。有了去中心化身份，用户才能在诸如元宇宙、Web3 体系中构建信任机制。

非同质化代币：是一种独特的基于区块链的可编程数字项目，可公开证明数字资产（如数字艺术或音乐）或标记化的物理资产（如房屋，汽车或文档）的所有权。这是和去中心化身份对应的“去中心化资产”，资产管理不再由统一的权威机构控制，而是交给区块链等信任机制，同时在资产确权、资产交易中保护用户隐私。

元宇宙：是一个集体虚拟 3D 共享空间，由虚拟增强的物理和数字现实的融合创建。元宇宙具备持久性，提供增强的沉浸式体验。元宇宙的核心在于数字映射，如何将现实场景数字化、虚拟化，这涉及到隐私保护交易、隐私保护应用、隐私保护建模、隐私计算网络、隐私边缘计算等许多隐私计算相关技术体系。

Web3：是一个新的技术栈，用于开发分布式的 Web 应用程序，使用户能够控制自己的身份和数据。数据的归属和使用都属于数据生产者用户本身，有效地缓解了隐私泄露等

数据安全问题，隐私计算在其中发挥了举足轻重的作用，如何在保障数据安全的同时充分发挥数据的价值，这是 Web3 依靠隐私计算的关键应用。

网络安全网格架构：是一种新兴的方法用来构建可组合的分布式安全控制，从而提高整体安全有效性。整个网络体系的安全是个庞大的课题，隐私计算在其中的角色可以理解为技术骨架，从网络节点的组建、网络通信的加密、网络数据的安全存储，都需要隐私计算保驾护航。

数据可观察性：是通过持续监控、跟踪、警报、分析和故障排除处理来了解组织数据环境、数据管道和数据基础架构运行状况的能力。数据的全生命周期管理，这恰是隐私计算目前主流的定义，数据从产生、存储、共享、利用、销毁，到潜在的泄露、结构破坏风险，都需要数据组织的管控，隐私计算是强有力的技术工具。

https://mp.weixin.qq.com/s/nrRJdB4tGJioCHToVtVgFw

2、《数字政府行业趋势洞察报告（2022 年）》：预计 2023 年政务云市场规模将达到 1203.9 亿元

近日，由中国信通院联合相关单位共同发布了《数字政府行业趋势洞察报告（2022 年）》，报告聚焦我国数字政府产业发展各环节，绘制产业全景，同时展望数字政府未来发展

趋势，旨在为我国数字政府的规划、建设、发展等环节提供参考。报告指出：预计 2023 年政务云市场规模将达到 1203.9 亿元。

从地方推进看，截至 2022 年 6 月，我国 31 个省（自治区、直辖市）和新疆生产建设兵团，超过五成地区已经发布了专门的数字政府战略规划文件，各地基本都成立了由政府一把手带队的数字政府建设领导小组统筹指导数字政府建设。另有若干省份在数字经济和智慧城市相关规划中提及数字政府建设要求。

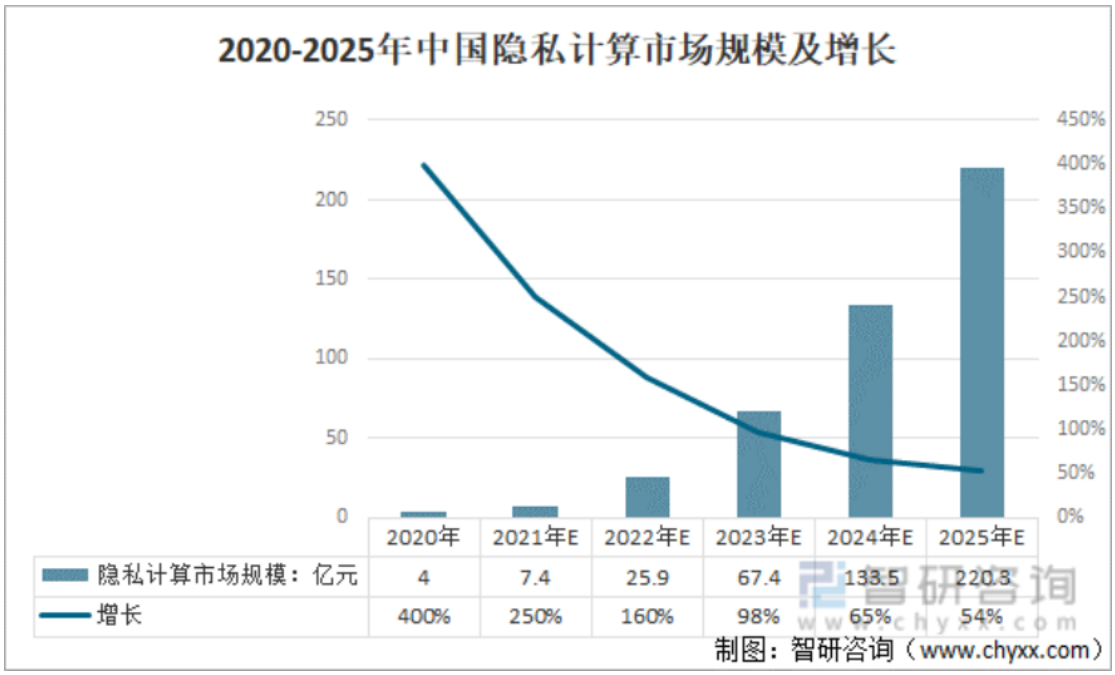
从市场规模看，我国数字政府市场规模保持高速增长，以政务云为例，2021 年，我国政务云市场规模达到 802.6 亿元，政务云作为资源整合共享、业务系统开发和部署的底座，未来仍将保持稳定增长态势，预计 2023 年市场规模将达到 1203.9 亿元。随着各地基础设施建设的逐步完善，数字政府进入到以深化应用和政府治理为导向的新阶段，政务数据、软件和服务市场份额将会持续扩大。

https://mp.weixin.qq.com/s/Tq4Pq09RXrDqCFWeqPexow

3、2021 年中国隐私计算市场规模

随着中国大数据产业发展以及隐私计算技术不断实现商业化，隐私计算技术产品蓬勃发展，形成一定优势，市场

规模将持续增长。目前数据使用方支出主要为产品及服务费，预计到 2025 年该领域市场将超过 200 亿，2021 年至 2025 年年均复合增长率达 133.4%。



资料来源：甲子光年、智研咨询整理

初创专精型厂商和人工智能/金融科技厂商是主力军。据统计，2021 年各领域隐私计算厂商中，锘崴科技等初创专精型厂商市场规模总量最高，占 31%；其次是平安科技等人工智能/金融科技厂商，占 22%；区块链厂商占 21%；百度等互联网厂商占 14%；星环科技等网络安全/大数据厂商占 10%。从聚焦行业来看，金融行业占比最高。

从中国隐私计算各行业市场规模占比来看，金融领域占 39%；政务领域占 28%；医疗领域占 22%；其他领域占 11%。通过对金融、政务、医疗领域隐私计算市场规模进行测算，

2021 年至 2025 年，年均复合增长率均在 130-150%左右，呈现高速增长态势。预计到 2025 年隐私计算金融领域市场规模 116.2 亿元，政务领域市场规模 61.6 亿元，医疗领域市场规模 59.5 亿元。

https://mp.weixin.qq.com/s/9PL4IKoJc7-vqX5UpuVbaw

4、单核 CPU 破解后量子加密候选算法只需一小时

鲁汶大学研究人员提出一种针对 SIDH 协议的高效密钥恢复攻击方法，使用普通单核 CPU，一小时即可攻破 SIKE 抗量子密码算法。

密钥封装机制是一种使用非对称密码学技术安全交换对称密钥的协议。SIKE (Supersingular Isogeny Key Encapsulation，超奇异同源密钥封装)是一种广泛应用的密钥封装机制，2022 年 7 月入选 NIST 后量子密码学算法第 4 轮。有多个工业实现和部署实验。相比对称密钥算法，目前使用的密钥封装易被量子计算机攻击。使用复杂数学构建的超奇异同源图被认为可以对抗量子计算机的攻击。

SIKE 协议的正确性和安全性依赖于 SIDH(Supersingular Isogeny Diffie-Hellman，超奇异同源 Diffie-Hellman)，即计算超奇异椭圆曲线间同源的困难性问题。SIDH 的安全性与寻找两条具有相同点数的超奇异椭圆曲线之间的同源映射问

题密切相关。

研究人员对攻击算法进行了实现——Magma，Magma 成功破解了 SIKEp434。Magma 分别在 4 分钟和 6 分钟内成功解决了微软 SIKE 挑战赛$IKEp182 和$IKEp217 问题。研究人员将 Magma 部署在 Intel Xeon CPU E5-2630v2（2.60GHz）单核 CPU 上，运行约 62 分钟即成功恢复 SIKEp434 参数（满足 NIST 后量子安全等级 level 1）。

https://mp.weixin.qq.com/s/tMbWlnusQhaYR74GsvYqsg

5、2022 年上半年报告了近 2,000 起数据泄露事件

在一份题为“数据泄露情报状况：2022 年中”的新报告中，安全公司 Flashpoint 着眼于 2022 年上半年报告的数据泄露的数量和类型。

到目前为止，今年上半年各组织已报告了 1,980 起违规事件。这比 2021 年上半年的销量低 15%左右，这似乎是一个积极的趋势。但是，数字可能具有欺骗性，尤其是因为组织不一定及时报告违规行为。

同期，泄露的记录数量从去年的 273 亿条大幅下降至今年的 14 亿条，这一下降是由于报告的开放式错误配置服务和数据库泄露事件减少。

2022 年上半年报告的大多数(60%)违规行为是由黑客

造成的，这在过去几年中一直是最常见的违规类型。大约 11% 的违规行为的原因尚不清楚，而其他违规行为是由病毒或欺诈引发的。在有明确原因的违规行为中，大约四分之一发生在受影响的组织内部，表明存在某种类型的内部威胁。其中，大多数（61%）归因于处理数据的错误。

https://www.techrepublic.com/article/almost-2000-data-breaches-reported-for-the-first-half-of-2022/?web_view=true

业界观点

1、冯登国院士：关键信息基础设施安全保护三大关键能力

《关键信息基础设施安全保护条例》自 2021 年 9 月 1 日起施行，即将实施一周年，值此之际，冯登国院士发表三点建议。

大力提升关键信息基础设施的弹性安全能力。要真正使得弹性安全技术落地生效，充分发挥其在关键信息基础设施安全保护中的重要作用，不能仅仅停留在口头上，要有检验弹性安全技术发挥效果的手段和方法，从而引导关键信息基础设施安全保护体系向着正确的方向发展。

要确实加强关键信息基础设施的数据安全治理能力。不仅要重视数据的存储和传输安全，也要重视数据的使用安全，更要重视数据的全生命周期安全。我们要重点围绕关键信息基础设施敏感数据的窃取、破解、篡改等攻击活动，确实加强数据安全防护和治理能力。

要高度重视新技术应用对关键信息基础设施带来的安全威胁风险评估能力，积极采取有效的应对措施，提升关键信息基础设施的对抗能力和防护水平。

https://mp.weixin.qq.com/s/smY0WuXqmG4sFzjsEIv8tg

2、邬贺铨：从实践中深化对数据中心“数学”与“算术”的认识

在 2022 中国算力大会主论坛上，中国工程院院士、中国互联网协会咨询委员会主任邬贺铨详细阐述了对数据中心“数学”与“算术”的思考。他解释道，“数学”指的是研究数据的科学，“算术”是研究算力的技术。

在以算为主还是以存为主方面，邬贺铨表示，人工智能驱动算力需求快速增长，基于 GPU 等构建的人工智能智算中心适于训练数据导出模型，训练出数学模型后，深度神经网络并不需要调度非常多的参数，降低了对算力的需求，基于 CPU 的通用算力的 IDC 适用于在已知数学模型下的计算任务。因此他表示，人工智能智算中心主要任务是算，IDC 互联网数据中心主要任务是存。

在基础算力、智能算力和超算三个算力里，美国分别占全球 35%、15%、30%，而中国分别占 27%、26%和 20%，美国是基础算力为主，中国智能算力的能力远超美国。中国的超算和智能算力基本以政府为主建设，基础算力以运营商和互联网企业为主。

在谈到东数西算时，邬贺铨表示，东数西算使算力设施的布局超越了数据中心枢纽的范畴，东部与西部互为冷热数据的配对方面，要有合适的比例。同时，同一数据中心枢纽

或集群内部也有很多比例需要优化。

https://mp.weixin.qq.com/s/AryX_BMeqUlbtlUKn08B8w

3、李苏：基层央行视角下的金融数据安全管理探索

近日，中国人民银行衡阳市中心支行李苏就金融行业的数据安全建设提出了见解。李苏认为金融行业数据安全管理面临的问题和挑战主要包括：数据安全管理体系不健全、数据治理能力参差不齐、开放融合和新技术应用进一步提高数据安全风险系数。对此，李苏提出建议：

构建全局的数据安全风险管理体系。强化风险识别，做到风险“可感”；深入分析研究，做到风险“可判”； 开展联防共治，做到风险“可控”。

以标准驱动数据能力建设。组织开展专题培训；强化标准宣贯力度；深化标准落地实施。

打牢数据融合应用的制度和技术基础。通过制定数据共享的制度和标准规范，实现数据交换流程标准化，数据交换过程“透明”化；探索建设省级数据交换平台，同时可引入沙盒监管机制解决因数据融合应用带来的未预测到的风险和不可控因素，实现规范、高效、统一、便于管理、安全可控的数据接入方式，推动省级金融服务系统数据互联互通，为接入全国一体化政务服务平台，加快跨机构、跨地域、跨行

业数据资源的共享提供基础支持；充分利用隐私计算技术、人工智能技术、自动化合规检查工具；落实责任加强监督管理。

https://www.secrss.com/articles/46020

4、杨殿阁：数据安全管理关乎智能汽车竞争胜负

近日，清华大学车辆与运载学院教授杨殿阁表示，智能汽车的发展需要靠数据驱动，数据迭代是智能汽车技术进步的生命线。

而智能汽车的数据来源非常复杂，既包括车载摄像头、激光雷达、毫米波雷达等感知的地理信息、交通信息、行人信息等外界环境感知数据，也包括驾驶员个人信息、车辆行驶轨迹、车载总线数据等车内数据。另外，手机与车机结合以后，在车上还会存储个人社交账号、支付密码、家庭信息、车架号等个人隐私数据。因此，智能汽车的数据安全涉及国家信息安全、个人隐私保护、车辆安全防护等多个方面。

因此，杨殿阁提出智能汽车数据安全管理建议：宜粗不宜细，采取“自上而下”和“自下而上”相结合的模式发展。在智能汽车技术尚处于探索阶段，国家“自上而下”统筹考虑定框架、定底线、确保数据安全的底线和边界，同时给予企业和行业一定的自由度，“自下而上”开展探索，大学、行业组

织和企业联合起来，在国家划定的底线和框架内，百花齐放，探索智能汽车数据的采集、存储、管理和使用的细节，探索如何最好发挥数据作用，有效驱动智能汽车技术的发展，探寻安全与创新发展的“度”。

https://www.tsinghua.edu.cn/info/1662/97357.htm

5、穆飞：数字化转型过程工作重点及挑战调研

近日，Forrester 调研数据显示,全球范围的两千多位受访者中,选择数据分析的受访者达到 34%;中国的 271 位受访者中,选择数据分析的比例达到了 44%,在所有选项中高居第一位。中国企业对数据问题是首要挑战的认可度高达 31%。这表明,数据分析已成为数字化转型过程中的重中之重,数据问题则是企业数字化转型的首要挑战。

提升数据管理水平,战略、技术、组织和流程,这几个维度缺一不可。从调研数据看,每个维度都存在诸多挑战。从调研数据看，每个维度都存在诸多挑战:

1）数据战略维度:79%受访者认为企业内部对于数据价值及资产缺乏统一认知与目标,难以有效协同。

2）技术维度:超过 75%的受访者表示企业现有数据基础设施技术水平无法充分利用多元化数据。82%受访者表示现有技术对半结构化以及非结构化数据关注不足。

3）数据孤岛:65%受访者表示,企业数字化业务不断新增的业务系统产生了新的数据孤岛。

http://science.china.com.cn/2022-08/17/content_42074166.htm

数据安全事件

1、印度金融服务公司 37,000 名用户的个人数据、交易详情在线泄露

2022 年 8 月 9 日，据外媒报道，印度金融服务公司数字支付系统平台 BharatPay 最近遭遇数据泄露事件，影响其后端数据库，其中包含大量客户的个人身份信息(PII)、财务余额和交易数据。这些泄露的数据范围从 2018 年 2 月到 2022 年 8 月，并在暗网论坛上发布出售。研究人员发现，除了这些泄露的 PII 数据外，BharatPay 的交易数据和在线账单支付服务商的 API 密钥以及几家 SMS 供应商的信息也被泄露。

https://izoologic.com/2022/08/18/indian-payment-platform-bharatpay-suffered-from-a-data-breach/

2、微软员工在 GitHub 上意外泄露内部敏感登录凭据

2022 年 8 月 18 日报道，微软的员工已暴露了公司在线基础设施的敏感登录凭据。该漏洞首先由网络安全研究公司 SpiderSilk 报告，随后由微软证实。文章称，暴露的数据来自 GitHub 上的员工。

SpiderSilk 首席安全官 Mossab Hussein 表示，源代码和

凭证泄露导致的事故变得越来越多，提前识别越来越困难。他说：“我们继续观察到意外的源代码和凭证泄露是公司攻击面的一部分，并且越来越难以及时准确地识别出来。这对当今大多数公司来说都是非常具有挑战性的问题。”

据获悉，Azure 是微软云计算机服务，类似于亚马逊 AWS 服务。泄露的凭据与微软官方 tenant ID 有关。tenant ID 是链接到一组特定 Azure 用户的唯一标识符。此次泄漏并未访问任何敏感数据，该公司已采取更安全措施来防止凭证共享。

https://www.ithome.com/0/635/707.htm

3、攻击 Twilio 的黑客暴露了 1900 名用户的 Signal 电话号码

2022 年 8 月 15 日报道，在本月初 Twilio 云通信公司遭受的数据泄露事件中，接近 1900 名 Signal 用户的电话号码被暴露。

Twilio 为 Signal 提供电话号码验证服务，上周披露，攻击者于 8 月 4 日入侵了其网络。这家通信公司证实，在黑客通过向 Twilio 员工账户发送带有恶意链接的短信获得访问权限后，属于其 125 名客户的数据被暴露。但是对于大约 1,900 名 Signal 用户来说，他们的电话号码可能会暴露给 Twilio

攻击者，攻击者可能试图将它们注册到另一台设备上。

https://www.bleepingcomputer.com/news/security/twilio-hack-exposed-signal-phone-numbers-of-1-900-users/

4、超 9,000 台 VNC 服务器在没有密码的情况下在线暴露

研究人员发现了至少 9,000 个暴露的 VNC（虚拟网络计算）端点，无需身份验证即可访问和使用，从而使威胁参与者可以轻松访问内部网络。

VNC（虚拟网络计算）是一个独立于平台的系统，旨在帮助用户连接到需要监控和调整的系统，通过网络连接通过 RFB（远程帧缓冲协议）提供对远程计算机的控制。

如果这些端点没有使用密码适当地保护，它们可以作为未经授权的用户的入口点，包括具有恶意意图的威胁参与者。根据暴露的 VNC 背后的系统，例如水处理设施，滥用访问权的影响可能对整个社区造成毁灭性的影响。

https://mp.weixin.qq.com/s/8WdX6VYwPLkxj7VOWHVY1A

5、航空航天和国防巨头遭受网络攻击，大量数据被窃取

2022 年 8 月 17 日，据外媒报道，黑客组织 Killnet 声称对航空航天和国防巨头洛克希德-马丁公司发动了一次大规模 DDoS 攻击。另外，该组织还表示从洛克希德-马丁公

司一名员工那里窃取了大量数据，并威胁要泄露这些数据。

Killnet 组织在其 Telegram 上分享了一段视频，声称已经窃取了包括姓名、电子邮件地址、电话号码和照片等在内的洛克希德-马丁公司员工个人信息。

https://mp.weixin.qq.com/s/O96xTkrZbxv1oBWofR21tA

6、CS:GO 最大交易平台遭黑客攻击，600 万美元游戏皮肤失窃

据媒体 8 月 16 日称，CS:GO（反恐精英：全球攻势）最大的皮肤交易平台之一 CS.MONEY 遭到攻击，在损失了价值约 600 万美元的 20000 件物品后下线。CS.MONEY 拥有 53 种武器的 1696 种独特皮肤，管理的总资产价值为 16500000 美元，在攻击事件后下跌到了 10500000 美元。据悉，攻击者通过某种方式获得了用于 Steam 授权的 Mobile Authenticator(MA)文件的访问权限，然后控制了 100 个包含该服务持有的皮肤的 bot 帐户，并进行了约一千笔交易。该平台已中断三天，但被盗物品仍未被找回。

https://www.bleepingcomputer.com/news/security/cs-go-trading-site-hacked-to-steal-6-million-worth-of-skins/

7、黑客利用 0-day 漏洞从比特币 ATM 中窃取加密货币

2022 年 8 月 20 日，据外媒报道，黑客利用 General Bytes 比特币 ATM 服务器中的 0-day 漏洞从客户那里窃取加密货币。当客户通过 ATM 存入或购买加密货币时，资金将被黑客吸走。General Bytes 是比特币 ATM 的制造商，根据产品的不同，它允许人们购买或出售 40 多种不同的加密货币。

https://www.bleepingcomputer.com/news/security/hackers-steal-crypto-from-bitcoin-atms-by-exploiting-zero-day-bug/

8、英国一水厂疑遭勒索软件攻击，IT 系统中断服务敏感数据或泄露

2022 年 8 月 17 日报道，英国南斯塔福德郡水务公司（South Staffordshire Water）是一家供水商，每天为 160 万消费者提供约 3.3 亿升饮用水。日前，该公司发表一份声明，确认 IT 系统已经因网络攻击而宕机。

据悉，此次攻击疑似为 Clop 勒索软件团伙所为。攻击恰逢英国消费者面临严重的缺水危机，目前英国国内已经有八个地区实施了供水配额和禁止私接软管等政策。网络犯罪分子当然不会随意选择目标，抢在严重缺水期间攻击供水商，有望迫使受害者面对巨大的民众用水压力而乖乖支付赎金。

Clop 表示已经成功接入水务公司的监测控制与数据采

集系统，甚至有能力操纵该系统对 1500 万客户造成损害，并从受感染的系统中窃取到 5TB 资料。

https://www.secrss.com/articles/45938

9、英特尔新型 CPU 漏洞可致敏感数据泄露

研究人员在英特尔 CPU 中发现了一个名为 ÆPIC 的新漏洞，该漏洞使攻击者能够从处理器中获取加密密钥和其他机密信息。ÆPIC 泄漏(CVE-2022-21233) 是第一个架构上的 CPU 错误，它可能导致敏感数据泄露并影响大多数第 10 代、第 11 代和第 12 代 Intel CPU。

据英特尔发布的公告显示：“某些英特尔® 处理器中的潜在安全漏洞可能允许信息泄露。英特尔正在发布固件更新以解决此潜在漏洞。”

https://mp.weixin.qq.com/s/0rn40GzfZaQJo4-hkHOklA

10、阿根廷科尔多瓦司法机构遭到 Play 团伙的勒索攻击

据媒体 8 月 15 日报道，阿根廷科尔多瓦司法机构在遭到 Play 团伙的勒索软件攻击后 IT 系统关闭。攻击发生在 8 月 13 日，系统和网络门户中断迫使员工使用笔和纸来提交官方文件。Clarín 报道称，攻击影响了司法机构的系统和数据库，是历史上针对公共机构最严重的攻击。虽然该机构尚

未披露此次攻击的细节，但有记者透露，加密文件添加了“.Play”扩展名，这可能与 2022 年 6 月开始活跃的新勒索团伙 Play 有关。

https://www.bleepingcomputer.com/news/security/argentinas-judiciary-of-c-rdoba-hit-by-play-ransomware-attack/