大数据协同安全技术
国家工程实验室
National Engineering Laboratory for Big Data Collaborative Security Technology

全球数据安全观察

总第 69 期 2021 年第 45 期

（2021.11.29-2021.12.05）

大数据协同安全技术国家工程实验室

目录

政策形势

1、工信部印发“十四五”大数据产业发展规划

2021 年 11 月 30 日，工业和信息化部印发《“十四五”大数据产业发展规划》，具体内容可以概括为“3 个 6”，即 6 项重点任务、6 个专项行动、6 项保障措施。

其中，6 项重点任务包括：**一是**加快培育数据要素市场；**二是**发挥大数据特性优势；**三是**夯实产业发展基础；**四是**构建稳定高效产业链；**五是**打造繁荣有序产业生态；**六是**筑牢数据安全保障防线。坚持安全与发展并重，加强数据安全管理，加大对重要数据、跨境数据安全的保护力度，提升数据安全风险防范和处置能力，做大做强数据安全产业，加强数据安全产品研发应用。

https://mp.weixin.qq.com/s/g8Hyo6b7ENr4U5DJEICjfg

2、《上海市数据条例》正式发布，2022 年 1 月 1 日起施行

据上海人大网站 11 月 29 日消息，《上海市数据条例》已由上海市第十五届人民代表大会常务委员会第三十七次会议于 2021 年 11 月 25 日通过，现予公布，自 2022 年 1 月 1 日起施行。《条例》施行后，上海还将制定数据分级分类保护、重要数据目录管理、数据安全管理等配套措施，落实

重要数据备案和数据安全评估制度。建立健全全流程数据安全管理制度，组织开展数据安全教育培训等。

https://mp.weixin.qq.com/s/gwTMwjTxC1auYTdiULQabw

3、央行发布《金融数据安全 数据安全评估规范》（征求意见稿）

据全国金融标准化技术委员会网站消息，《金融数据安全 数据安全评估规范》（征求意见稿）已发布并公开征求意见。据了解，该标准适用于金融业机构开展金融数据安全评估使用，并为第三方安全评估机构等单位开展金融数据安全检查与评估工作提供参考。

https://mp.weixin.qq.com/s/ds3uKwkamh881sqnRwiG_Q

4、《福建省“十四五”数字福建专项规划》发布

近日，福建省政府印发《福建省“十四五”数字福建专项规划》（下称《规划》）。《规划》明确：到2025年，福建省基本实现数字政府智治化、数字经济高端化、数字社会智慧化、数据要素价值化，成为数字中国建设样板区。到2035年，基本实现现代化数字强省远景目标。

《规划》提出六大重点任务：打造协同高效的数字政府、发展融合创新的数字经济、建设共治共享的数字社会、构建

赋智赋能的数据体系、布局集约智能的新型基础设施、**筑牢可信可靠的网络安全屏障**。

https://mp.weixin.qq.com/s/jdTPAcZcznQhIeoUYxM4_A

5、网约车等交通新业态反垄断监管将加大，严查“大数据”杀熟

2021 年 11 月 30 日，交通运输部等多部门发布“关于加强交通运输新业态从业人员权益保障工作的意见”，明确提出将加大反垄断监管力度，防范资本在交通新业态领域无序扩张，**严查“大数据”杀熟等行为**，并督促网约车平台在驾驶员和车辆新注册时，应要求提供网约车驾驶员和车辆许可证件，对无法提供的不予注册。

https://www.bjnews.com.cn/detail/163824364814364.html

业界观点

1、数据防勒索的三个最佳实践

除新冠肺炎疫情之外，勒索软件已成为全球经济面临的严重威胁之一。Gartner 的调查研究数据表明，企业遭遇攻击早已不再是“会否”的问题，而只是“何时”的问题。

面对勒索软件挑战，我们可以创建经济高效的多层策略：1）重视可见性与审计，关键在于知道哪些数据是经常使用的热数据，而哪些是不经常使用的冷数据；2）创建多层数据管理防御，包括热数据快照与备份、冷数据云分层和不可变存储；3）制定计划并加以验证，记录和测试计划，确保能通过快速恢复和替代数据访问方法来保护数据，这样才能在不中断业务或支付大笔赎金的情况下保持业务正常运行。

https://mp.weixin.qq.com/s/PUsW4isaDkEih_htlqoHag

2、做好数字化组织的“首席安全官”——构建有效落地的网络安全一体化防御体系

近些年，在监管单位推动的网络安全实战化攻防演练和重大安保的持续“淬炼”下，验证了很多关键信息基础设施单位网络安全保障体系的好与坏。几场攻防战下来，但凡在优秀行列的单位无不体现了核心三要素，强有力的网络安全

组织，领导重视和优秀的安全负责人（如安全处长、安全总监或者首席安全官）。

数字化企业需要一个成熟务实的首席安全官。第一，具备识别业务发展、信息化建设和网络安全同步调的能力；第二，具备三个常态化核心能力，即汇报、横向协同、一体化落地；第三，具备一体化弹性可扩展的网络安全业务管理和技术平台能力。

https://mp.weixin.qq.com/s/7Qm0ytIG20kg_NxazSXWUw

3、联邦学习技术应用思考：需求还是方法？

目前，“联邦学习”这个术语在市场上存在很多认识上的误解和混淆，主要原因是其既在广义上表达了保护数据前提下联合多方数据训练模型的需求，又在狭义上表示了一类通过暴露部分数据信息来提升训练性能的方法。有趣的是，作为广义上的需求，它强调为了保护数据安全，可以牺牲部分准确性；但作为狭义的方法，它反而强调通过牺牲安全来换取性能提升。

因此，作为行业用户，选择是不是存在“联邦学习”的需求（也叫做数据融合计算、数据价值流通的需求），是一个纯粹的业务问题，其判断标准是数据价值流通能否带来业务价值；在这一需求基础上，是不是要选用狭义的“联邦学

习”方法和系统来满足这个需求，是个纯粹的 IT 技术和安全合规问题，需要考虑和平衡的是数据的敏感性、泄露的代价，和进行数据保护所需的技术成本。

https://mp.weixin.qq.com/s/K4uIV-c9q3Zp55g6C4Ip1g

4、遭遇双重勒索软件攻击的受害者飙升 935%

研究人员记录了双重勒索攻击的同比增长 935%，超过 2300 家公司的数据发布在勒索软件勒索网站上。Group-IB 的 2021/2022 年高科技犯罪趋势报告涵盖了 2020 年下半年至 2021 年上半年的时期。它声称，在此期间，初始访问经纪人和勒索软件即服务 (RaaS) 附属计划的 “邪恶联盟”导致违规行为激增。

Group-IB 指出，总的来说，勒索软件数据泄漏站点上的违规受害者数量从上一个报告期内的 229 人激增至 2371 人。同期，泄漏站点数量增加了一倍多，达到 28 个，RaaS 附属公司的数量增加了 19%，发现了 21 个新团体。

https://www.infosecurity-magazine.com/news/double-extortion-ransomware-soar/

5、《“十四五”大数据产业发展规划》解读之陈兵：需建立数据要素动态权属制度和全国统一市场

11 月 30 日，工信部发布《“十四五”大数据产业发展规划》(下简称《规划》)，在延续“十三五”规划关于大数据产业定义和内涵的基础上，进一步强调了数据要素价值。其中，在加快培育数据要素市场方面，《规划》提到要建立数据要素价值体系、健全数据要素市场规则、提升数据要素配置作用。

当前数据要素市场化配置还面临两方面问题：首先，数据权属制度不完善，影响数据要素市场公平竞争。其次，统一的数据要素市场尚未建立，阻碍数据要素有序流通。为此，应尽快在法治框架下建立以“数据相关行为”为基准的数据要素动态权属制度，分阶段、分步骤构建全国统一有序开放的数据要素市场，为推动数据要素公平竞争与有序流通、实现数据要素市场化配置奠定基础。

构建统一开放的数据要素市场，具体而言，应着力从以下四个方面进行安排部署，分阶段、分步骤实现数据要素市场建设：第一，探索建立数据要素全国统一市场。第二，做好数据要素标准化建设的顶层设计。第三，推进政府数据科学有序开放。第四，建立统一的数据治理机构。

https://mp.weixin.qq.com/s/t33iXBzqMbPw0n25a-GEHw

安全事件

1、洛杉矶计划生育协会 (PPLA) 在勒索软件攻击后披露数据泄露

2021 年 12 月 1 日，据外媒报道，洛杉矶计划生育协会（Planned Parenthood Los Angeles）在 10 月份遭受勒索软件攻击后披露了一起数据泄露事件，该攻击暴露了大约 400000 名患者的个人信息。

根据发送给洛杉矶计划生育协会 (PPLA) 患者的数据泄露通知，网络攻击发生在 10 月 9 日至 17 日之间，攻击者可以从受感染的网络中窃取文件，文件包含患者的个人信息，包括他们的地址、保险信息、出生日期和临床信息，例如诊断、程序和/或处方信息。

https://www.bleepingcomputer.com/news/security/planned-parenthood-la-discloses-data-breach-after-ransomware-attack/

2、松下集团发生严重数据泄漏

2021 年 11 月 30 日，据报道，松下集团确定，攻击者在入侵期间已经访问并获取了文件服务器上的一些重要数据。日前，日本跨国企业集团松下披露遭遇网络攻击并发生数据泄漏，原因是未知的威胁行为者访问了其服务器。松下表示：

“公司已确认网络于 2021 年 11 月 11 日被第三方非法访问，作为内部调查的结果，确定攻击者在入侵期间已经访问并获取了文件服务器上的一些重要数据。”

https://www.secrss.com/articles/36659

3、美 DNA 检测公司敏感数据泄露影响 210 万用户

2021 年 11 月 30 日，据报道，位于美国俄亥俄州费尔菲尔德进行 DNA 检测服务的 DNA 诊断中心 (DDC) 披露了一起数据泄露事件，黑客设法访问了用户的高度敏感的个人数据，包括支付卡数据。其中超过 210 万 (2102436) 名客户/用户的敏感个人和财务数据被黑客窃取。

https://www.wangan.com/p/7fy74777ea2c020f

4、MonoX 宣布因漏洞导致被黑客窃取 3100 万美元

2021 年 12 月 2 日，据外媒报道，区块链初创公司 MonoX Finance 由于软件中用于起草智能合约部分存在漏洞，已经被黑客已经成功窃取了 3100 万美元。该公司使用一种被称为 MonoX 的去中心化金融协议，让用户在没有传统交易所的一些要求的情况下交易数字货币代币。

https://www.cnbeta.com/articles/tech/1209969.htm

5、黑客从 BadgerDAO DeFi 平台窃取了 1.2 亿美元的加密货币

2021 年 12 月 3 日报道，黑客从连接到去中心化金融平台 BadgerDAO 的多个加密货币钱包中窃取了价值 1.2 亿美元的各种代币。攻击者能够在 BadgerDAO 网站的 UI 中注入恶意脚本，从而拦截和劫持 Web3 交易。资金在攻击者的控制下被劫持到钱包中。

https://securityaffairs.co/wordpress/125242/cyber-crime/badgerdao-defi-platform-hack.html