[公开]360NELab-DST-0-044-20210531

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 44 期 2021 年第 20 期

（2021.05.24-2021.05.30）

大数据协同安全技术国家工程实验室

目录

安全事件

1、印度航空泄漏 450 万旅客数据，波及多家航空公司

2021 年 5 月 24 日报道，在 2021 年 2 月旅客服务系统提供商 SITA 被黑客入侵两个多月后，印度航空公司首次通告泄漏了大约 450 万旅客的个人信息。数据泄漏事件涉及 2011 年 8 月 26 日至 2021 年 2 月 3 日之间注册的个人数据，其中包括姓名、出生日期、联系信息、护照信息、机票信息、星空联盟和印度航空的飞行常客数据（但没有密码数据）以及信用卡数据。

https://mp.weixin.qq.com/s/iE0A46NaIMnWpxndSm0Y1Q

2、印尼的国家医疗保险计划泄露了至少 100 万公民的档案

2021 年 5 月 24 日，印度尼西亚通信和信息技术部承认，运营国家健康保险计划的机构泄露了 100 万份记录。

https://www.theregister.com/2021/05/24/indonesia_health_data_breach/

3、加拿大邮政 95 万客户信息遭泄漏

2021 年 5 月 27 日，加拿大邮政公司(Canada Post)软件供应商遭到黑客攻击，有 95 万以上的客户信息遭到泄漏破坏。

泄漏的数据属于 2016 年 7 月至 2019 年 3 月之间近三年时间的信息，其中 97%是包裹收件人的姓名和邮政地址，其余 3%包括电子邮件地址和电话号码。

https://www.bleepingcomputer.com/news/security/canada-post-hit-by-data-breach-after-supplier-ransomware-attack/

4、日本多个政府部门遭遇黑客攻击，大量数据泄漏

2021 年 5 月 27 日，黑客近日攻击了富士通公司开发的信息共享平台 ProjectWEB，窃取了多个日本政府机构的数据。受影响的日本政府包括国土、基础设施、运输和旅游部、内阁秘书处，此外还包括成田国际机场。

https://www.bleepingcomputer.com/news/security/japanese-government-agencies-suffer-data-breaches-after-fujitsu-hack/

5、跨国物流公司卑尔根 Bergen 客户数据泄露

2021 年 5 月 25 日报道，最近，国外 IT 安全研究人员发现了一个属于 Bergen Logistics（卑尔根）的暴露数据库，该数据库存储了 467979（46 万）条与他们的货运和客户相关的记录。这意味着与卑尔根开展业务的任何客户或在美国境内从卑尔根收到包裹的任何人都可能受到此数据泄漏的影响。

https://mp.weixin.qq.com/s/DKZEEBadqqkxf-FgFmyuXg

政策形势

1、2021 中国国际大数据产业博览会 5 月 26 日开幕

5 月 26 日，2021 中国国际大数据产业博览会（简称“2021 数博会”）在贵州省贵阳市开幕。2021 数博会由中国国家发展和改革委员会、中国工业和信息化部、中国国家互联网信息办公室、贵州省人民政府主办，围绕“数据创造价值 创新驱动未来”大会主题，以“数智变 物致新”为年度主题，采取线上线下相融合的办会模式，开展“一会、一展、一发布、大赛及系列活动”。会议为期三天，共举办 26 场高端对话及论坛。

https://mp.weixin.qq.com/s/5k_1vIGW4HzRvqiC-F241g

2、2021 数博会“围绕数字经济创新·共建数据安全生态”论坛成功举办

5 月 26 日，2021 数博会“围绕数字经济创新·共建数据安全生态”论坛在贵阳国际生态会议中心成功举办。

本次论坛由中国国际大数据产业博览会组委会主办，中国网络空间安全协会、全国工商联大数据运维（网络安全）委员会、大数据协同安全技术国家工程实验室、贵州大数据安全工程研究中心承办，贵阳经济技术开发区管理委员会、

360 科技集团有限公司、阿里巴巴集团、数据安全认证（贵州）有限公司、数据观（北京）传媒科技有限公司协办。

https://mbd.baidu.com/newspage/data/landingsuper?context=%7B%22nid%22%3A%22news_9497281419904954957%22%7D&n_type=-1&p_from=-1

3、四部门联合印发《全国一体化大数据中心协同创新体系算力枢纽实施方案》

5 月 24 日，国家发改委、中央网信办、工业和信息化部、国家能源局联合印发《全国一体化大数据中心协同创新体系算力枢纽实施方案》（以下简称《实施方案》），明确提出构建国家算力网络体系。

《实施方案》提出“**试验多方安全计算、区块链、隐私计算、数据沙箱等技术模式，构建数据可信流通环境，提高数据流通效率。**”给出了当前突破数据流通瓶颈的技术路径——促进以隐私计算为代表的数据流通技术的应用。

https://mp.weixin.qq.com/s/jjxoKx6ROJFMDrJRVIlX2w

4、上海召开数据立法研讨会，《上海市数据条例（暂定名）》草案已经形成

2021 年 5 月 27 日，上海市召开数据立法研讨会，全国

人大财经委、国务院办公厅、兄弟省市、上海市相关部门、高校、科研机构、企业代表等100余位嘉宾参会，就加快突破数据立法中的重点、难点问题展开探讨。上海数据立法起草组组长、市大数据中心主任朱宗尧表示，《上海市数据条例（暂定名）》草案已经形成，这部《条例》草案在不触碰数据权属的前提下，依据现行《民法典》和正在审议中的《个人信息保护法》有关立法内容和精神，从确认各方主体可以对数据行使哪些权利的角度，对数据主体和数据处理者的“数据权益”作出了明确规定，明确市场主体在不违反法律、行政法规禁止性规定以及与被收集人约定的情况下，对自身产生和依法收集的数据，以及开发形成的数据产品和服务，有权进行管理、收益和转让，解决权益不清带来的数据流通不畅、利用不足的问题。

https://mp.weixin.qq.com/s/6mUncTw77ymLr4VWkY7UfA

5、德国通过电信行业数据和隐私保护新法

近期，德国议会通过了一项关于电信和电信媒体的数据保护和隐私的法律（简称TTDSG），这是立法者首次将欧盟关于Cookies的要求从电子隐私指令中移植过来。通过该法律，德国的数据保护规定将得到统一，并与欧盟的《通用数据保护条例》（GDPR）保持一致。

https://mp.weixin.qq.com/s/Qck-PHnD1WFvFGWdgF03og

6、《深圳数据条例（草案）》提请“二审”，进一步保护用户隐私和个人信息

《深圳经济特区数据条例（草案修改一稿）》日前提请市人大常委会会议“二审”，**条例草案进一步加强了对用户隐私的保护 ，明确规定，自然人有权随时拒绝用户画像和个性化推荐。**

https://mp.weixin.qq.com/s/gKKWF_SFAWBixi8JgNRV5g

业界观点

1、2021 数博会|360 周鸿祎：从勒索攻击“APT 化”窥见城市安全能力体系建设

“数字时代披着勒索软件外衣的定向攻击本质上是国家级高级可持续威胁攻击（APT 攻击）。”在 5 月 26 日 2021 中国国际大数据产业博览会上，360 创始人、董事长周鸿祎发表主题演讲时表示，要帮助国家、城市、行业、企业构建网络安全基础设施体系，综合提升应对数字威胁的网络安全能力。这种有组织的、持续性的、长时间的勒索攻击在不断迭代进化中向“APT 化”演进，周鸿祎提出五大趋势：

一是定向攻击将成为常态，撒大网式勒索攻击正在变少，针对高价值目标的定向攻击越来越多。攻击者会根据目标的支付能力、对加密数据的依赖程度以及攻击可能造成的政治、经济上的影响精心选择目标；

二是勒索软件也更加专业化，攻击手法不断翻新，传播途径更加多样化，如供应链传播等；

三是持续渗透潜伏成为常用手法，攻击者通过前期对选定目标相关信息的收集，持续渗透，找出薄弱攻击面，实现致命一击；

四是勒索软件团伙呈现出更强的组织性，不同犯罪组织相互配合，形成更广泛的犯罪生态；

五是勒索软件攻击走向产业化，勒索即服务成为攻击新模式，攻击者只需要购买勒索服务就可以发起攻击，门槛极低。

面对未来高智商攻击团队发起的持续性网络攻击，传统的碎片化手段已经失效，因此亟需构建一套新的安全能力体系。为此，周鸿祎呼吁抛弃过去各自为战的思路，在国家、城市、行业、企事业单位建立以安全大脑为核心的数字安全能力体系。

https://mp.weixin.qq.com/s/dmrDIO7vSWO3aDpcH9SEwA

2、中国信通院发布《数据价值化与数据要素市场发展报告（2021 年）》

5 月 27 日，中国信息通信研究院副总工程师史德年在“2021 中国国际大数据产业博览会”上发布了《数据价值化与数据要素市场发展报告（2021 年）》。

报告建立了数据价值化的“三化”框架，即数据资源化、数据资产化、数据资本化。目前全球尚处于数据资源化的初级阶段，数据采集、数据标注有望成为撬动产业规模发展的新引擎。我国数据要素市场正在形成包含数据交易主体、数据交易手段、数据交易中介、数据交易监管的“四位一体”发展格局。

https://mp.weixin.qq.com/s/sWXAG72gAiPyYzlagXulug

3、零信任四化之应用零信任化的趋势分析

未来零信任发展会呈现明显的“四化”特征，即应用零信任化、传统网络安全产品零信任化、零信任技术协议标准化和零信任落地成熟度评估模型化。

自零信任概念提出以来，经过长时间的发展和实践，零信任构架理论已经趋向完善，获得了包括安全厂商、企业 CTO 及应用开发厂商的广泛认可，应用零信任化趋势逐渐清晰。

（1）服务隐藏。传统的边界防护理念中，应用需要在网络边界暴露业务端口，从而给不法人员提供了可以攻击的目标。零信任采用单包认证（SPA）的方式，业务服务端口对外不可见，非法攻击将失去攻击的入口，从而保护应用安全。

（2）零信任身份验证与授权。零信任网络不再设置可信的网络边界，采用主动防御的方式，只有信任评估为合法的请求才允许访问业务服务，且持续进行动态验证，非法攻击将无法穿透到业务服务上。

（3）贴近化网关。相比于传统网络边界所定义的内网可信区域，零信任框架将内网服务识别为不可信，通过贴近化网关将内网业务服务器进行微隔离，只有可信的身份和权限才能访问授权的业务服务资源，从而实现各应用服务之间的零信任化。

（4）基于信任评估的访问控制。零信任的信任评估机制，结合了包括用户环境、网络、角色及权限、用户行为等全面的因素进行综合安全评估，根据应用安全要求，提供与风险评估结果一致的访问权限。

https://www.freebuf.com/articles/network/272858.html

4、勒索软件威胁现状

对组织和个人用户来说，勒索软件是一个持续的严重安

全威胁。作为一种恶意工具，它的设计越来越精妙，传播能力更强，面向人群更广，适用于各种攻击人群。

经过多年发展，勒索软件已然成熟，即便是技术小白也可以轻易上手。同时，出现了许多变种，用于勒索软件即服务（RaaS）。

当前，勒索软件攻击的主要目标是政府机构和医疗、教育及运输行业的关键系统。勒索软件将会长期存在，随着RaaS 的出现，威胁范围还可能会扩大。频繁的离线备份、持续的用户意识培训以及对系统和网络安全的增强都有助于检测和防护勒索软件。

https://www.freebuf.com/news/272568.html