[公开]360NELab-DST-0-064-20211101

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 64 期 2021 年第 40 期

（2021.10.25-2021.10.31）

大数据协同安全技术国家工程实验室

目录

政策形势

1、注册数据安全官（CDSO）培训正式开课

2021 年 10 月 26 日-29 日，由大数据协同安全技术国家工程实验室举办的注册数据安全官（CDSO）培训班于北京正式开课。本次培训采用线下面授方式，吸引了来自政府、运营商、高校、金融等多个行业的主管部门领导、数据安全管理者以及数据安全从业者参与。

https://mp.weixin.qq.com/s/eh7P4KVAW2rdZwK_XBVrUw

2、《中华人民共和国个人信息保护法》11 月 1 日起施行

《中华人民共和国个人信息保护法》在 11 月 1 日起正式施行。作为中国首部针对个人信息保护的专门性立法，个人信息保护法将进一步强化个人信息安全监管与治理，把个人信息使用权关进法律的笼子里。

https://xhpfmapi.xinhuaxmt.com/vh512/share/10329252?channel=weixin

3、网信办《数据出境安全评估办法 (征求意见稿)》公开征求意见

2021 年 10 月 29 日，为了规范数据出境活动，保护个人

信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，依据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，国家网信办就《数据出境安全评估办法（征求意见稿）》公开征求意见。

http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm

4、《上海全面推进城市数字化转型“十四五”规划》发布

“十四五”时期是上海推动城市整体迈入数字时代，全面构筑未来城市新形态、战略新优势的关键阶段。为进一步推动城市数字化转型，上海市于近期编制了《上海市全面推进城市数字化转型“十四五”规划》（以下简称《规划》）。

《规划》明确了“十四五”时期上海城市数字化转型的“1+4”目标体系。总体目标是：到 2025 年，上海全面推进城市数字化转型取得显著成效，对标打造国内一流、国际领先的数字化标杆城市，国际数字之都建设形成基本框架，为 2035 年建成具有世界影响力的国际数字之都奠定坚实基础。

围绕上述目标，《规划》提出了“1+3+6”的任务体系。其中，“1”是厚植一个转型基础，完善城市 AIoT（人工智能物联网）基础设施，构建城市数据中枢体系，打造城市共性技术赋能平台，加快推动城市形态向数字孪生演进。“3”是三

化联动推进转型，包括以经济数字化转型助力高质量发展，以生活数字化转型创造高品质生活，以治理数字化转型实现高效能治理。“6”是实施六大工程，包括“数字价值提升、数字技术策源、数字底座赋能、数字规则引领、应用场景共建、转型标杆示范”工程，为城市全面数字化转型提供坚实的支撑。

https://mp.weixin.qq.com/s/mhNnl_cSAt93-D64UJudTA

5、《广东省公共数据管理办法》正式印发

10 月 25 日，广东省人民政府官网公布《广东省公共数据管理办法》（以下简称《办法》）。作为广东省首部省级层面关于公共数据管理的政府规章，《办法》将于 11 月 25 日起正式实施。其中有诸多制度创新，**包括国内首次明确将公共服务供给方数据纳入公共数据范畴、首次在省级立法层面真正落实“一数一源”、首次明确数据交易标的等。**

《办法》还**在省级层面首次确立数据主体授权第三方使用的机制**。基于此，广东省正积极探索以公共数据资产凭证化助推数字经济发展。今年 10 月 16 日，广东开出全国首张公共数据资产凭证，接下来，通过首轮公共数据资源普查汇聚的 285 亿条“公共数据，都有望被彻底激活。

https://mp.weixin.qq.com/s/7WNAsRvuQzebVim18s-HJQ

业界观点

1、Gartner：2021-2022 年 8 大网络安全预测

隐私法案、勒索软件攻击、信息物理系统和董事会级别审查，逐渐成为安全和风险负责人需要优先关注的事项。Gartner 分析师预测，未来几年将出现更多的权利下放、监管措施和安全问题。应当将以下战略规划设想纳入未来一年的路线规划：

（1）到 2023 年底，现代隐私法案将涵盖全球 75%人口的个人信息;（2）到 2024 年，采用网络安全网格（cybersecurity mesh）架构的组织，将把安全事件对财务造成的影响平均降低 90%；（3）到 2024 年，30%的企业将采用来自同一供应商的云交付安全 Web 网关（SWG）、云访问安全代理（CASB）、零信任网络访问（ZTNA）和防火墙即服务（FWaaS）功能；（4）到 2025 年，60%的组织将把网络安全风险作为进行第三方交易和业务往来的主要决定因素；（5）到 2025 年底，通过立法来规范勒索软件的赎金支付、罚款和谈判的民族国家比例将上升至 30%，而 2021 年这一比例还不到 1%；（6）到 2025 年，40%的董事会将会设立专门的网络安全委员会，并由一名具备资质的董事会成员监督；（7）到 2025 年，70%的首席执行官将要求建立组织弹性文化，以应对同时来自网

络犯罪、恶劣天气事件、国内动乱和政治动荡的威胁；（8）到 2025 年，威胁行为者会成功地将运营技术环境武器化，足以造成人员伤亡。

https://www.secrss.com/articles/35533

2、NIST 发布 2020 年网络安全和隐私年度报告，聚焦 9 大领域

2021 年 9 月 30 日，美国国家标准与技术研究院(NIST)发布了《2020 年网络安全和隐私年度报告》。NIST 强调，NIST 信息技术实验室(ITL)网络安全和隐私计划成功应对了安全和隐私方面的众多挑战和机遇。

报告分为九个优先领域，包括：网络安全意识和教育；身份和访问管理；度量和测量；风险管理；隐私工程；新兴技术；密码标准和验证；值得信赖的网络和值得信赖的平台。

https://www.secrss.com/articles/35426

3、2021 年上半年全球高级持续性威胁（APT）研究

2021 年上半年，全球高级持续性威胁（APT）整体形势依然严峻，发现和披露的 APT 攻击活动较去年同期大幅增加。上半年全球公开报告数量 492 篇，**其中披露的攻击活动涉及 APT 组织 90 个**，首次披露的组织 17 个，无论报告数

量还是组织数量都已超去年同期。**从全球范围看，APT 攻击活动还是重点关注政治、经济等时事热点。目标主要针对政府、国防军工、科研等行业领域。**今年全球疫情仍然肆虐，局部地区疫情形势相比去年甚至更加严峻，围绕“新冠疫情”开展的相关攻击活动继续处于高位。上半年攻击活动中利用的 0day 漏洞数量已超过去年全年总和，达到历史新高。上半年爆发的针对美国最大燃油管道运营商和爱尔兰卫生服务部门在内的一系列针对关键基础设施的勒索攻击事件，体现出勒索攻击不断 APT 化的发展趋势。勒索威胁逐渐上升到事关国家安全的层面，已成为全球网络安全的共同挑战。

https://cert.360.cn/report/detail?id=6c9a1b56e4ceb84a8ab9e96044429adc

4、依法依规，筑牢汽车数据安全处理防线

开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等，无论是单独处理、协同处理，都应严格遵守法律法规各项要求。例如，汽车制造商为实现汽车功能，引入了软件供应商协同处理视频音频。在这种情况下，符合《个人信息保护法》中共同处理情形的，服务方可以约定各自的权利和义务，但是，该约定不影响个人向其中任何一个个人信息处理者要求

其遵守法律法规各项要求、履行个人信息保护的义务和责任。

https://mp.weixin.qq.com/s/A8pTQEGc42j3SJaNd2zSyA

5、政务信息共享中的数据安全技术要求框架实践思路

国家支持政务数据开放共享，但数据开放共享的前提是规范与安全。数据共享方需盘点共享数据资产，进行数据分类分级，最终形成数据开放目录供外界请求使用，同时数据共享需建立政务数据开放平台，平台需规定统一的共享数据申用规范，约束政务数据开放行为，平台还需配备相关数据安全管理制度与防护技术，监测政务数据开放共享过程中的数据安全风险，及时进行数据安全风险管控。

政务数据共享安全建设，应遵循统筹协调、分级保护、权责统一、安全可控的原则，以制度规范为指引，以技术防护为抓手，以运行管理为保障，从战略规划、管理制度、防控技术与综合运营 4 方面构建政务数据共享、开放的闭环管理，全面推动政务数据共享安全体系建设落地，确保政务数据安全。

https://mp.weixin.qq.com/s/RUIemnJ3YIL1BgBfaCcE2Q

安全事件

1、攻击者从 Cream Finance 窃取了价值 1.3 亿美元的加密货币资产

Cream Finance 是一种去中心化借贷协议，供个人、机构和协议访问金融服务。2021 年 10 月 28 日，攻击者从 Cream Finance 去中心化金融(DeFi)平台窃取了价值 1.3 亿美元的加密货币。

https://securityaffairs.co/wordpress/123861/cyber-crime/cream-finance-cyber-heist-130m.html

2、54 亿条个人信息在暗网出售

近日，无锡警方成功破获了一起侵犯公民个人信息案，犯罪团伙非法获取医疗、出行、快递等公民信息，数据累计高达 54 亿多条，并通过"暗网"平台提供查询、出售服务。

https://view.inews.qq.com/a/20211026A08AIZ00

3、全国首例非法获取地理信息数据刑事案在湖州宣判

近日，浙江省湖州市中级人民法院宣判了全国首例非法获取地理信息数据刑事案，二审维持了三被告人分别被判处三年六个月至一年四个月不等有期徒刑，并处罚金 10 万元

至 2 万元不等的裁判结果。

法院经审理查明，2019 年 9 月至 2020 年 8 月，被告人张某、陈某未经 Q 公司允许，擅自使用陈某编写的 XCORS.GwServer 程序等技术手段，通过搭建中间平台的方式，获取 Q 公司等精确定位差分系统的数据用于转发。经鉴定，该 XCORS.GwServer 程序具有避开 Q 公司账号认证、位置识别、处置转发行为等安全技术措施的功能。

https://mp.weixin.qq.com/s/qVcOjSXF3aTigZ8CJDjgzQ

4、泰国豪华连锁酒店报告数据泄露

据 ZDNet10 月 28 日报道，泰国一家豪华连锁酒店报告了一起数据泄露事件，原因是臭名昭著的网络罪犯团伙在最近几周发动了一系列攻击。

Desorden Group 声称他们是针对 Centara Hotels & Resorts 发起攻击的幕后黑手。除了对 Centara Hotels & Resorts 的黑客攻击外，Desorden 还声称入侵了 Central Group 的服务器。该集团在泰国拥有连锁酒店和 2000 多家餐厅。这次泄漏涉及 80GB 的文件，包括客户的个人信息和每家餐厅的业务详细信息。

https://www.163.com/dy/article/GNH3SKN50552BJIM.html

5、伊朗加油站因遭到网络攻击而停止服务

2021 年 10 月 26 日，伊朗的加油站系统遭受了一次网络攻击，导致全国多地加油系统停止服务。此外，多处户外电子广告牌上信息也被篡改。

此次受影响的是伊朗国家石油产品分销公司（NIOPDC），在全国有 3500 多处加油站点，攻击的主要目标是旗下享受政府补贴价格的加油管理系统。伊朗最高网络空间委员会主席阿博哈桑·菲鲁扎巴迪 (Abolhassan Firouzabadi)表示，这些攻击很可能是由国家支持的，但具体确定是哪个国家还为时过早。目前尚未有国家或组织声称对这起事件负责。

https://www.freebuf.com/news/293125.html