[公开]360NELab-DST-0-062-20211018

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 62 期 2021 年第 38 期

（2021.10.11-2021.10.17）

大数据协同安全技术国家工程实验室

目录

政策形势

1、信安标委《汽车采集数据处理安全指南》

2021 年 10 月 11 日，信安标委发布了《汽车采集数据处理安全指南》（以下简称“《指南》”），《指南》规定了对汽车采集数据进行传输、存储和出境等处理活动的安全要求。《指南》明确了其适用于汽车制造商开展汽车的设计、生产、销售、使用、运维，也适用于主管监管部门、第三方评估机构等对汽车采集数据处理活动进行监督、管理和评估。

https://mp.weixin.qq.com/s/mrZV_0TmtnBPFbkm0ytaFQ

2、贵州省上线数据流通交易平台，已完成第一笔实质数据交易

通过贵州省数据流通交易平台，云上北斗（贵州）科技股份有限公司作为“买方”，向“数据商”北京帝测科技股份有限公司购买了贵阳市城区倾斜摄影数据产品，交易金额 225 万元。随着第一笔实质数据交易撮合完成，贵州新的大数据交易中心正式“开所”运行。

作为抢抓国家数据要素市场培育新机遇、落实“在实施数字经济战略上抢新机”要求的具体举措，近日，贵州省数据流通交易服务中心挂牌成立，**采用隐私计算、联邦学习、**

区块链等新技术手段，以安全可信的开发利用环境为底座，搭建贵州省数据流通交易平台。10 月 11 日，数据流通交易平台上线运行，标志着贵州数据流通交易进入 2.0 时代。

https://mp.weixin.qq.com/s/AQl1BhxvAORhXi_TXiqgmQ

3、广东开出全国首张公共数据资产凭证

2021 年 10 月 16 日，广东开出全国首张公共数据资产凭证，数据要素市场化配置改革率先破局。广东针对数据资产化过程中存在的确权难、监管难、跨域互信难等问题，提出“以凭证承载资产、以凭证声明权益、以凭证治理数据、以凭证保障合规”的公共数据资产凭证解决方案，加快盘活数据资源，释放数据红利。

https://mp.weixin.qq.com/s/I8oWrvrBpQ6mPK43SBEDKw

4、意大利部委委员会通过意大利数据保护法修正案

意大利部委委员会宣布通过一项法令，其中包含与数据保护法相关的紧急条款。部委委员会概述了法令法将对个人数据保护法规定的要求进行一些修订，其中包含使国家立法适应一般数据保护条例（GDPR）中对出于公共利益目的处理个人数据的有关规定。

https://www.dataguidance.com/news/italy-council-ministries-

adopts-amendments-italian-data

5、甘肃：深入打造数据基座，推动政务数据开放共享

近日，甘肃省人民政府印发了《关于加强数字政府建设的意见》，提出要深入打造数据基座，推动政务数据开放共享，包括加强数据统筹管理、建设数据资源库、升级改造数据共享交换平台和推动数据要素开放共享等措施。

https://mp.weixin.qq.com/s/UWM7ajqJizoNmi7kzvviWQ

业界观点

1、美财政部：2021 年上半年支付勒索软件赎金金额已超过 2020 全年

根据美国财政部当地时间 10 月 15 日发布的一份报告，截至今年6月，金融机构已经向金融犯罪执法网络报告了635起与勒索软件相关的可疑活动，比 2020 年报告的所有活动增加了 30%。勒索软件支付成本也在大幅度攀升。2021 年报告的总价值为 5.9 亿美元，平均每月 6640 万美元，而 2020 年全年的总价值为 4.16 亿美元。网络保险公司的数据表明，勒索软件攻击不仅变得越来越频繁，而且成本也越来越高，遭勒索且索赔的案件也呈上升趋势。

https://www.secrss.com/articles/35189

2、Forrester：2025 年应用安全市场规模将达 129 亿美元

Forrester 刚刚发布报告《应用安全解决方案预测，2020-2025 年（全球）》，预测了八个应用安全子市场的增长率，并发现：

运行时保护将比安全扫描增长更快。应用安全工具分为两大类：安全扫描工具和运行时保护工具。Forrester 预计，在容器安全和机器人（Bot）管理的带动下，运行时保护市场

的增长速度将略高于安全扫描市场。然而，安全扫描市场不会停滞不前--我们预测，在未来五年内，软件成分分析（SCA）、交互式应用安全测试、静态应用安全测试和动态应用安全测试都将经历两位数的增长，其中 SCA 将处于领先地位。

容器安全将拥有最快的增长。2021 年预测更新中加入了容器安全工具，因为对容器的投资大幅增加，企业把可扩展性、敏捷性和降低成本作为投资最大的好处。容器的普及推动了容器安全投入，Forrester 预计，在未来五年内，容器安全市场将拥有最高的保护技术投资增长率。

机器人管理将超越传统的 WAF。Forrester 预测，网络应用防火墙（WAF）的许多核心功能将被机器人管理所取代，使其在 2025 年超过传统 WAF，成为核心应用保护解决方案。机器人管理可以检测和防止一系列基于 Bot 的攻击，包括凭证填充、网页抓取、库存囤积/锁单和影响力欺诈。机器人管理工具保护应用程序免受不良机器人的影响，同时允许良性的机器人，并确保正常用户不被不必要的验证码和挑战所阻碍。

https://www.secrss.com/articles/35109

3、《2021 年中国网络安全产业分析报告》发布

2020 年我国网络安全市场规模约为 532 亿元，由于受疫

情影响，2020 年网络安全市场规模增速放缓，同比增长率为 11.3%。《数据安全法》的发布实施将进一步激发数据安全市场需求；《个人信息保护法》和《关键信息基础设施安全保护条例》等关键政策的发布将引领新需求并将形成可观的增量市场，预计未来三年将保持 15%+增速，到 2023 年市场规模预计将超过 800 亿元。

https://mp.weixin.qq.com/s/Mo3fffsX7am7EwSPSZW0xA

4、大数据 2.0 时代，贵州数据安全怎么办？

面向未来，当数字经济和大数据产业发展进入发展期，当前的主要问题已经**从“有多少数据”变成“能不能用好数据”的 2.0 时代**，这时候，数据安全问题给这个新阶段带来的挑战愈发明显，解决好数据安全问题让数据能够用起来，变得更加迫切。

全球发达地区都开始全面转向用安全能力成熟度的思路应对网络安全挑战，而在数据安全领域，我国有最好的条件并且走在了前面，从 2015 年开始推出数据安全能力成熟度的理念，推出了数据安全能力成熟度模型标准（DSMM），2017 年开始一直在做大量实践。现阶段伴随着 DSMM 的推广，应该加大对数据安全官和数据安全工程师的培养，以更综合性的人才应对越发复杂的数据安全局势。数据安全人才

不仅是技术性人才，也要懂得相关标准、政策、业务和理念等。

http://jgz.app.todayguizhou.com/news/news-news_detail-news_id-11515115751436.html

5、Gartner《2021 安全运营技术成熟度曲线》解析

Gartner 发布《Hype Cycle for Security Operations, 2021》（2021 安全运营技术成熟度曲线），对主流的安全运营技术进行了解读，相较于 2020 年，数字化转型加速了企业与 IT 信息技术的关联。

Gartner 依其专业分析预测与推论各种新科技的成熟演变速度及要达到成熟所需的时间，具体可分为：**技术萌芽期、期望膨胀期、泡沫破裂谷底期、稳步爬升复苏期、生产成熟期** 5 个阶段。在 2021 年报告中，萌芽阶段包括自主渗透测试和红队服务、外部攻击面管理（EASM）、网络资产攻击面管理（CASSM）、渗透测试即服务（PTaaS）、扩展检测和响应（XDR）技术；膨胀阶段包括数字风险保护服务（DRPS）、漏洞优先排序（VPT）、文件分析技术（FA）、托管检测和响应 (MDR) 服务、威胁情报（TI）服务、网络威胁检测及响应（NDR）、 运营系统（OT）安全技术；破裂阶段包括集成化的风险管理（IRM）、安全编排自动化响应（SOAR）、欺骗平

台（DP）、入侵与攻击模拟（BAS）技术；复苏期包括端点检测与响应技术（EDR）、基于硬件的安全技术、安全信息和事件管理（SIEM）、云访问安全代理（CASB）技术；成熟期包括漏洞评估（VA）技术。

https://mp.weixin.qq.com/s/YSYc6bzbJd-cb30-tOmA3Q

安全事件

1、美国奎斯特诊断公司承认 35 万名患者医疗资料被泄露

2021 年 10 月 13 日报道，奎斯特诊断公司向美国证券交易委员会(SEC)通报称，公司旗下生育诊所 ReproSource 在八月份遭到了勒索软件攻击，约 350,000 名患者的大量健康信息和财务信息遭到泄漏，部分患者的社会安全号码（ssn)和信用卡号码也遭到泄漏。

与其他关键基础设施一样，医疗保健系统面临着勒索软件攻击的独特脆弱性，因为暴露的数据不仅会影响患者的隐私，还会影响他们对医疗的选择。而勒索软件还在持续对生育诊所和其它卫生系统进行攻击，获取着宝贵又重要的数据。

https://www.secrss.com/articles/35066

2、厄瓜多尔最大银行业务因遭遇勒索攻击被迫中断

2021 年 10 月 14 日报道，上周末，因遭遇网络攻击，厄瓜多尔最大私营银行皮钦查银行关闭了部分网络和系统，业务被迫中断，此次攻击导致该银行业务大面积中断，ATM 机、网上银行、移动客户端、数字渠道和自助服务、电子邮件均无法运行。有消息人士称，这是一起勒索软件攻击，攻击者还在该银行网络上安装了 Cobalt Strike 信标。

https://www.secrss.com/articles/35108

3、巴西电子商务服务商泄露近 18 亿条个人记录

2021 年 10 月 14 日报道，据研究人员称，一家巴西电子商务公司在错误配置 Elasticsearch 服务器后无意中暴露了近 18 亿条记录。错误配置的 Elasticsearch 服务器未进行加密，更没有密码保护，它包含 610GB 的数据，包括客户的全名、家庭和送货地址、电话号码和帐单明细。还暴露了卖家的全名、电子邮件和公司/家庭地址、电话号码和公司/税号(CNPJ/CPF)。

https://www.secrss.com/articles/35113

4、欧盟拟向 Facebook 开罚单，最高 2.71 亿人民币

2021 年 10 月 14 日消息，爱尔兰数据保护委员会（Data Protection Commission，简称 DPC）提议欧盟向 Facebook 开出罚单，最高 3600 万欧元（约 2.71 亿人民币）。

DPC 提交的决定草案认为，Facebook 没有提供有关其根据“接受服务条款”进行数据处理的法律依据，并指出 Facebook 所提供的信息相互脱节。因此，Facebook 违反了 GDPR 第 5(1)(a)、12(1)和 13(1)(c)条,应对其处以 2800 万至 3600 万欧元的罚款。

https://mp.weixin.qq.com/s/LSZkufC8D5R7IlYXSMUfKg

5、宏碁服务器再次被窃，超 60GB 用户数据或被出售

2021 年 10 月 15 日报道，宏碁服务器数据再次被窃，该公司数百万客户和客户的数据目前被扣押。超过 60GB 的委托人、客户和零售商的信息现在掌握在黑客手中，他们正在寻找买家出售这些数据。 此次泄密主要影响印度的客户，这是宏碁在过去七个月里遭遇的第二次黑客攻击。前一次是在 3 月份，据 REvil 黑客组织声称，那次攻击涉及创纪录的 5,000 万美元赎金。

https://www.cnbeta.com/articles/tech/1190881.htm