[公开]360NELab-DST-0-031-20210222

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 31 期 2021 年第 7 期

（2020.02.08-2021.02.21）

大数据协同安全技术国家工程实验室

摘要

本期全球数据安全观察搜集到的重要事件的主要类型为**数据泄露、勒索软件**和**数据安全政策以合规问题**。

1. Kroger 数据泄露暴露了药房和员工数据
2. 美国医院成千上万的病人档案泄露
3. 红杉资本风险投资公司披露数据泄露
4. 新加坡电信巨头近 13 万客户信息遭泄露
5. 2020 年美国医疗机构数据泄露造成 130 亿美元损失
6. 加密浏览器 Brave 被曝隐私漏洞
7. 黑客窃取信用卡数据，滥用 Google 的 Apps 脚本
8. 起亚汽车遭遇了 2000 万美元的勒索软件攻击
9. 多市遭勒索软件攻击后出现数据泄露
10. 美国议员提出《促进数字隐私技术法》法案
11. Facebook 因合规问题被罚 700 万欧元
12. 瑞典某警方违反该国刑事数据法被开出高额罚单

此外，在数据安全技术与观点方面主要讨论了：

1. 2020 数字经济展望：增强数据访问、共享和重用
2. EDPS 对《数字服务法》和《数字市场法》发表意见
3. 发展大数据不应牺牲个人信息保护，推动国家大数据立法时机已成熟

4. 国资委下发通知，加快推进国有企业数字化转型
5. 到 2025 年，全球数据中心市场将投资 4321.4 亿美元
6. 支持隐私保护的数字签名技术
7. 智能制造数据层风险分析与防护思考

全球动态

1. Kroger 数据泄露暴露了药房和员工数据

2021 年 2 月 20 日，超市巨头克罗格（Kroger）遭受了数据泄露，此前用于安全传输文件的服务遭到黑客入侵，威胁者偷走了文件。该违规暴露了人力资源数据和药房记录。

https://www.bleepingcomputer.com/news/security/kroger-data-breach-exposes-pharmacy-and-employee-data/

2. 美国医院成千上万的病人档案泄露

2021 年 2 月 8 日，美国 11 家医院患者和员工的个人信息被黑客曝光，包含患者姓名、地址、生日、医疗诊断以及保险公司记录等信息在内的数万条记录被公布在网上。

https://www.infosecurity-magazine.com/news/tens-thousands-files-leaked-us/

3. 红杉资本风险投资公司披露数据泄露

2021 年 2 月 20 日，最著名的风险投资公司之一红杉资本（Sequoia Capital）披露了数据泄露事件。该公司告知投资者，未经授权的第三方可以访问其个人和财务信息。

https://securityaffairs.co/wordpress/114831/hacking/sequoia-cap

ital-data-breach.html

4. 新加坡电信巨头近 13 万客户信息遭泄露，涉身份证号等

2021 年 2 月 18 日报道，近日，新加坡知名电信公司新电信（Singtel）表示，已完成针对第三方文件共享系统漏洞的初步调查——约有 12900 名客户的个人信息遭到泄露，含身份证号等信息。去年 2 月，新电信曾因旗下应用发生信息泄露而被罚款 9000 新币。

https://www.secrss.com/articles/29328

5. 2020 年美国医疗机构数据泄露造成 130 亿美元损失

近日，据 Bitglass 的数据显示，去年美国的医疗保健数据泄露事件数量呈两位数倍数增长，受影响的人数超过 2600 万人。报告显示，与 2019 年的数据相比，泄露事件增加了 55％以上，达到 599 起违规事件。其中，最主要的原因来自外部攻击者的“黑客和 IT 事件”。与其他原因类别相比，此类数据占整个泄露记录的 91％以上。

https://mp.weixin.qq.com/s/abeUCNaV5ZzilC35jDdxlA

6. 加密浏览器 Brave 被曝隐私漏洞，向 DNS 服务器泄露用户匿名访问信息

2021 年 2 月 19 日，据报道，加密浏览器 Brave 被曝存在隐私漏洞，用户使用匿名浏览模式 Tor 时，会将访问信息泄露给 DNS 服务器。随后，开发团队回应称漏洞存在于浏览器的广告拦截组件中，目前该漏洞已修复。

https://www.freebuf.com/vuls/263891.html

7. 黑客窃取信用卡数据，滥用 Google 的 Apps 脚本

2021 年 2 月 19 日，攻击者滥用 Google 的 Apps Script 商业应用开发平台来窃取电子商店中的支付卡信息。攻击者使用 *script.google.com* 域避免检测并绕过内容安全策略（CSP）控件，默认情况下，电子商店的 CSP 配置中将 Google 域及其子域列入白名单。

https://securityaffairs.co/wordpress/114750/cyber-crime/googles-apps-script-magecart.html

8. 起亚汽车遭遇了 2000 万美元的勒索软件攻击

近日报道，目前为止，起亚汽车美国公司已经公开承认了他们的汽车发生了 "长时间的系统中断"，勒索软件团伙 DoppelPaymer 声称在攻击中已经加密锁定了该公司的文件，

并要求支付 2000 万美元的赎金。

https://www.4hou.com/posts/22gJ

9. 多市遭勒索软件攻击后出现数据泄露

2021 年 2 月 18 日，针对广泛使用的支付处理器 ATFS 的勒索软件攻击引发了加利福尼亚和华盛顿众多城市和机构的数据泄露通知。暴露的潜在数据因城市或代理商而异，但可能包括名称、地址、电话号码、车牌号、VIN 编号、信用卡信息、扫描的纸质支票和帐单详细信息。

https://www.bleepingcomputer.com/news/security/us-cities-disclose-data-breaches-after-vendors-ransomware-attack/

10.美国议员提出《促进数字隐私技术法》法案

美国参议员 Catherine Cortez Masto 于 2021 年 2 月 5 日宣布，她与美国参议员 Deb Fischer 和两名众议员一起提出了《促进数字隐私技术法》的第 224 号参议院法案。特别是，SB 224 法案会要求美国国家科学基金会(下称 "国家科学基金会")促进对提升私隐技术的研究，并制定标准，将提升私隐技术融入公共和私营部门的数据使用。具体来说，SB 224 会要求国家科学基金会支持以下方面的研究：在保持公平、准确和效率的前提下，对数据集中的个人资料进行去身份识

别、假名化、匿名化或模糊化的技术。在收集、存储、共享或汇总数据时用于保护个人隐私的算法和其他类似数学工具；技术，促进数据收集、共享和分析中的数据最小化原则。

https://mp.weixin.qq.com/s/EkI_8oqeuVXW29B3D0mTtg

11.Facebook 因合规问题被罚 700 万欧元

2021 年 2 月 17 日，意大利反托拉斯机构 AGCM(Autorità Garante della Concorrenza e del Mercato)向 Facebook 开具 700 万欧元罚单，以惩罚其数据实践的不合规。AGCM 发现 Facebook 误导用户对基于不同目的个人数据使用中“一般和不完整”信息的理解，包括定向广告等。

https://mp.weixin.qq.com/s/QknqUD6wANX81sTKb1E_vw

12.瑞典数据监督机构因违法使用 Clearview AI 向警方开出高额罚单

2021 年 2 月 18 日报道，瑞典数据保护机构 IMY 对该国一间警察局罚款 250 万瑞典克朗（30 多万美元），原因是其非法使用有争议的面部识别软件 Clearview AI 的行为违反了该国的刑事数据法。

https://mp.weixin.qq.com/s/-mP_uqvfptiI9tOHWjNX_A

业界观点

1. OECD 2020 数字经济展望：增强数据访问、共享和重用

近日，经合组织（OECD）发布《2020 年数字经济展望》报告，从数字化时代政策制定的综合方法、政策趋势、访问和连接、数字理解、使用和技能、增强数据访问、共享和重复使用、隐私和数据保护、数字安全、数字化转型中的消费者政策、数字化创新和不断发展的商业模式十个方面，展望了数字经济的前景。该报告指出，新冠疫情强化了对推动数字化转型的包容性需求，数据的访问、使用、创新、就业、社会、信任和市场开放将推动全方位的数字化转型。

https://mp.weixin.qq.com/s/-nIHV_OW0eVgzhEG6L7Yfw

2. EDPS 对《数字服务法》和《数字市场法》发表意见

2021 年 2 月 10 日，欧洲数据保护监督员（EDPS）公布了对欧盟委员会《数字服务法》和《数字市场法》提案的意见。关于《数字服务法》，EDPS 建议当涉及到内容审核、在线平台使用的在线定向广告和推荐系统时，应采取额外的措施保护个人权益。关于《数字市场法》，EDPS 认为创造一个有竞争力的数字市场是非常重要的，这将为公民提供更

多的在线平台和服务选择；基于用户对其个人数据更好控制权可以强化数字市场的竞争力。

https://mp.weixin.qq.com/s/QknqUD6wANX81sTKb1E_vw

3. 发展大数据不应牺牲个人信息保护，推动国家大数据立法时机已成熟

当前，我国大数据运用飞速发展，数字经济保持高速增长态势，成为推动经济增长的重要引擎。据中国信息通信研究院统计，我国数字经济增加值已由 2011 年的 9.5 万亿元增加到 2019 年的 35.8 万亿元，占 GDP 比重从 20.3％提升到 36.2％。但是，大数据的应用在提高社会运转效率的同时，也带来了个人隐私泄露和数据权属不清晰等问题，大数据发展亟待一部国家专项立法来保驾护航。

https://mp.weixin.qq.com/s/fM9rfvTh1s6ve9QthX6-TQ

4. 国资委下发通知，加快推进国有企业数字化转型

近日，国务院国资委正式印发《关于加快推进国有企业数字化转型工作的通知》，系统明确国有企业数字化转型的基础、方向、重点和举措，开启了国有企业数字化转型的新篇章，积极引导国有企业在数字经济时代准确识变、科学应变、主动求变，加快改造提升传统动能、培育发展新动能。

https://mp.weixin.qq.com/s/piqmcpeKv78wRlwTmWFQzg

5. 到 2025 年，全球数据中心市场将投资 4321.4 亿美元

据安全研究机构 Frost & Sullivan 的分析发现，全球持续的高水平技术部署将导致数据创建的激增，推动对数据处理和存储能力的需求。其结果将会导致从企业到大型云的大量数据中心建设。预计到 2025 年，全球数据中心市场将投入 4321.4 亿美元，高于 2019 年的 2447.4 亿美元，复合年增长率为 9.9%。

https://mp.weixin.qq.com/s/7OZcWEpO0Wu14BsJ7WSi7A

6. 支持隐私保护的数字签名技术

数字签名是公钥密码体制下解决身份认证与内容认证问题的重要密码学技术手段。为了在传统数字签名的基础上实现身份匿名或内容隐藏等隐私保护需求，**群签名、环签名、盲签名等支持隐私保护的特殊数字签名算法得到了深入的研究和广泛的应用探索**。不仅实现了传统的基本认证功能，还能实现**有监管身份匿名、无监管身份匿名**以及**内容隐藏**。

https://www.freebuf.com/articles/database/259084.html

7. 智能制造数据层风险分析与防护思考

数据驱动制造是智能制造的必要条件，数据已成为增强制造业竞争力的关键要素。因此，数据安全也成为智能制造安全的重中之重，其贯穿各层面安全保障。从数据全生命周期看，各环节都存在安全风险。此外，人工智能、5G、数字孪生、虚拟现实等新技术应用引入新的数据安全风险隐患，如利用人工智能技术进行数据伪造、数据污染等。根据智能制造面临的设备、控制、网络、平台、数据等层面的安全风险分析，亟需建立针对性、体系化的智能制造网络安全防护框架。要从“全层面防护、自适应动态防护、协同联动防护”三个方面进行设计，因此，智能制造网络安全防护应建立各方协同、多方联动的合力，从管理、技术等角度构建协同联动安全防护体系。

https://www.secrss.com/articles/29373