[公开]360NELab-DST-0-056-20210823

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 56 期 2021 年第 32 期

（2021.08.16-2021.08.22）

大数据协同安全技术国家工程实验室

目录

政策形势.....1
1、《个人信息保护法》获通过，11 月 1 日起施行.....1
2、《关键信息基础设施安全保护条例》9 月 1 日起施行....1
3、国家互联网信息办公室等五部门发布《汽车数据安全管理若干规定（试行）》.....2
4、国家医保局：推动规范、高效、安全的数据交换和信息共享机制.....2
5、贵州将搭建公共资源交易区块链数据共享平台.....3
业界观点.....5
1、《个人信息保护法》十大亮点解读.....5
2、《关键信息基础设施安全保护条例》发布：将带来百亿级增量市场.....5
3、勒索软件攻击数量和赎金要求数额双双暴涨.....6
4、调查：零信任或将成为主流安全方案.....7
5、加强平台监管促进数据安全管理.....8
安全事件.....9
1、巴西国库局遭勒索软件攻击.....9
2、FBI 恐怖分子观察名单被曝光，内含 200 万条记录.....9
3、美国电信巨头 T-Mobile 遭遇重大安全事件，超 1 亿用户数据泄露.....9
4、Hive 勒索软件攻击 Memorial 卫生系统，窃取患者数据.....10
5、英国教育巨头培生因掩盖数据泄露被罚款 100 万美元.....10

政策形势

1、《个人信息保护法》获通过，11 月 1 日起施行

2021 年 8 月 20 日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》。个人信息保护法自 2021 年 11 月 1 日起施行。其中明确：①通过自动化决策方式向个人进行信息推送、商业营销，应提供不针对其个人特征的选项或提供便捷的拒绝方式②处理生物识别、医疗健康、金融账户、行踪轨迹等敏感个人信息，应取得个人的单独同意③对违法处理个人信息的应用程序，责令暂停或者终止提供服务。

http://www.xinhuanet.com/2021-08/20/c_1127779295.htm

2、《关键信息基础设施安全保护条例》9 月 1 日起施行

2021 年 8 月 17 日，国务院总理李克强日前签署国务院令，公布《关键信息基础设施安全保护条例》（以下简称《条例》），自 2021 年 9 月 1 日起施行。

《条例》建立专门保护制度，明确各方责任，提出保障促进措施，有利于进一步健全关键信息基础设施安全保护法律制度体系。

《条例》明确，重点行业和领域重要网络设施、信息系统属于关键信息基础设施，国家对关键信息基础设施实行重

点保护，采取措施，监测、防御、处置来源于境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治违法犯罪活动。

http://www.xinhuanet.com/2021-08/17/c_1127769001.htm

3、国家互联网信息办公室等五部门发布《汽车数据安全管理若干规定（试行）》

国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部联合发布《汽车数据安全管理若干规定（试行）》（以下简称《规定》），自 2021 年 10 月 1 日起施行。国家互联网信息办公室有关负责人表示，出台《规定》旨在规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，促进汽车数据合理开发利用。

https://mp.weixin.qq.com/s/OI8Q3fF97rNbQasX6qDKgw

4、国家医保局：推动规范、高效、安全的数据交换和信息共享机制

在保护个人隐私的前提下，打破“信息孤岛”，实现医保数据资源的共享，是推动我国医保保质量发展的方向之一。近日，国家医保局《国家医疗保障局关于政协十三届全国委

员会第四次会议第 0719 号（医疗体育类 066 号）提案答复的函》中，围绕“**推进共享医保数据**”的相关问题给出了方向。

目前《医疗保障法》已在公开征求意见阶段。征求意见稿第 47 条、第 52 条和第 66 条明确了医疗保障行政部门应当规范数据管理和应用权限，保护信息和数据安全，并对相关人员泄漏信息行为依法处理。下一步，国家医保局将做好以下几方面工作：一是**加快建设全国统一的医疗保障信息平台**，实现编码标准“纵向全贯通、横向全覆盖”。二是加强顶层设计，依法依规探索商业健康保险信息平台与全国统一的医疗保障信息平台**信息共享机制**，强化医疗健康大数据应用。

https://mp.weixin.qq.com/s/1riqojCdnEAC01KUgrDY0g

5、贵州将搭建公共资源交易区块链数据共享平台

8 月 16 日，省公共资源交易中心正式印发《贵州省公共资源交易区块链数据共享工作试点实施方案》，明确在国家信息中心、省人民政府办公厅、省大数据管理局的指导下，省级及各市（州）公共资源交易中心要充分发挥区块链的**数据一致存储、难以篡改、可追溯**等技术优势，让**交易过程更可信、交易数据更安全、交易服务更便捷**，并完成试点建设目标及各项任务。

根据方案，到 2021 年底，贵州要建成省公共资源交易区

块链数据共享平台，建立健全数据信任机制和数据确权管理机制，解决公共资源交易领域数据“确认难、运用难、管理难”的问题，实现贵州省公共资源交易数据防篡改、可追溯、可信任的管理应用，推动优化公共资源交易服务、强化交易管理支撑，打造便捷的移动应用场景，实现全省数字证书移动互认、链上金融服务及链上市场主体库等应用，为全国公共资源交易数据转型提供借鉴经验。

https://mp.weixin.qq.com/s/jtSg0A89oS2FTIQnJGaCZw

业界观点

1、《个人信息保护法》十大亮点解读

经过三次审议，8 月 20 日，十三届全国人大常委会第三十次会议表决通过了个人信息保护法，将于 2021 年 11 月 1 日起施行。全国人大常委会法工委经济法室副主任杨合庆 20 日对个人信息保护法进行了权威解读。

亮点一：确立个人信息保护原则；亮点二：规范处理活动保障权益；亮点三：禁止“大数据杀熟”规范自动化决策；亮点四：严格保护敏感个人信息；亮点五：规范国家机关处理活动；亮点六：赋予个人充分权利；亮点七：强化个人信息处理者义务；亮点八：赋予大型网络平台特别义务；亮点九：规范个人信息跨境流动；亮点十：健全个人信息保护工作机制。

https://www.secrss.com/articles/33669

2、《关键信息基础设施安全保护条例》发布：将带来百亿级增量市场

中国政府网 17 日发布《关键信息基础设施安全保护条例》（简称《条例》）。**《条例》提出，国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于**

中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯罪活动。

中信证券认为，《条例》要求对关键信息基础设施实行重点保护。根据我国现行的网络安全等级保护制度，预计保护等级不会低于三级，将带来巨大增量市场。

通过测算，中信证券预计《条例》带来的安全投入规模将达到百亿级。推荐处于估值底部，在政府、电信等行业需求提升下充分受益的安全公司。

目前，我国网络安全投入在 IT 整体预算中的占比仅为 1.84%，远低于美国（4.78%）和全球（3.74%）的水平。

https://www.secrss.com/articles/33542

3、勒索软件攻击数量和赎金要求数额双双暴涨

安全公司 Barracuda 本周发布的报告围绕勒索软件威胁的各个方面提供了一些新的见解。过去 12 个月里，30%的赎金要求高达 3000 万美元，但尝试谈判的受害者能够大幅降低赎金。从 2020 年 8 月到 2021 年 7 月，这家安全公司的研究人员识别并分析了总共 121 起勒索软件攻击，同比增长 64%。其中 30%的事件所涉赎金要求超过 3000 万美元，6%的事件所涉赎金要求甚至高达 5000 万美元之多。

Barracuda 和其他多家安全供应商指出，最近几个月，勒索软件攻击数量大幅增多。7 月，SonicWall 报告称，相比 2020 年上半年,今年上半年勒索软件攻击数量增长了 151%。SonicWall 在今年第二季度录得近 1.89 亿起勒索软件攻击，为其史上最糟情况。总体上看，安全供应商在 2021 年上半年记录的勒索软件攻击尝试达 3.047 亿之多，而 2020 年全年也就 3.046 亿而已。SonicWall 称，该攻击量使 2021 年有望成为勒索软件史上最糟糕的一年。

https://www.secrss.com/articles/33527

4、调查：零信任或将成为主流安全方案

近日，一项调查数据显示，零信任作为供应商推动的无边界安全策略，已经在企业中逐渐流行起来。

报告显示：“76%的企业正在实施零信任架构，比去年增加了 6%；新型冠状病毒加速了线下向混合工作模式的转变，也推动了零信任的更广泛采用，81%的企业已经开始转向混合工作场所。”

报告指出，采用零信任的主要原因包括提高安全性和合规性敏捷性、威胁检测和修复的速度以及安全分析的简单性和可用性。

https://www.aqniu.com/industry/76639.html

5、加强平台监管促进数据安全管理

随着平台经济的高速发展，人们在享受“数据红利”的同时，也同样面临“数据风险”的严峻挑战：数据泄露和滥用降低用户共享意愿；互联网设施关键节点存在数据安全隐患；数据跨境流动与数字主权问题日益凸显。

我国的平台经济正处于关键的发展时期，要从构筑国家竞争新优势的战略高度出发，明确规则，划清底线，加强监管，更好地统筹发展和安全、国内和国际的关系，强化平台企业数据安全责任。需要完善平台经济监管法律规范；探索数据驱动的弹性监管和柔性治理模式；加强平台企业海外上市的前置审查；建设国家级大数据平台推进数据的开放共享；设立国家类“数据银行”保障国家数据安全；将平台企业监管融入证券市场发行机制。

https://mp.weixin.qq.com/s/0fMLo9_WwQ-FNccThCebCQ

安全事件

1、巴西国库局遭勒索软件攻击

2021 年 8 月 18 日，据报道，巴西政府发表声明称该国的国库局上周五遭勒索软件攻击，表示立即采取了措施遏制网络攻击的影响，初步评估未发现国库局的结构系统有任何损坏。安全专家正对此进行分析。此次事件被认为是至今对巴西政府公共部门最庞大的一次网络攻击。

https://www.solidot.org/story?sid=68585

2、FBI 恐怖分子观察名单被曝光，内含 200 万条记录

2021 年 8 月 16 日，一个包含 190 万条记录的秘密恐怖分子观察名单在互联网上曝光，其中包括机密的“禁飞”记录。该列表可以在没有密码的 Elasticsearch 集群上访问。190 万条记录集包含有关人员的敏感信息，包括姓名、国籍、性别、出生日期、护照详细信息和禁飞状态。

https://www.bleepingcomputer.com/news/security/secret-terrorist-watchlist-with-2-million-records-exposed-online/

3、美国电信巨头 T-Mobile 遭遇重大安全事件，超 1 亿用户数据泄露

2021 年 8 月 16 日报道，美国电信巨头 T-Mobile 遭遇了

一起重大安全事件，生产环境被打穿，超 106GB 敏感数据失窃，超过 1 亿用户的个人信息被泄露售卖。攻击者声称，此举是为了对美国进行报复，打击美国的基础设施。8 月 17 日，T-Mobile 已确认黑客窃取了属于 4860 万现在和过去的用户记录。

https://www.secrss.com/articles/33478

4、Hive 勒索软件攻击 Memorial 卫生系统，窃取患者数据

2021 年 8 月 16 日，据外媒报道，Memorial Health System 是一个非营利性综合卫生系统，拥有 3000 多名员工。遭受了来自 Hive 勒索软件团伙的攻击后，系统计算机被加密，并已有证据表明攻击者窃取了包含 20 万名患者敏感信息的数据库，其中包含患者社保号、姓名和出生日期。

https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/

5、英国教育巨头培生因掩盖数据泄露被罚款 100 万美元

2021 年 8 月 16 日，美国证券交易委员会 (SEC) 宣布，英国跨国教育出版服务公司培生（Pearson），已就 2018 年数据泄露事件中披露程序处理不当的指控达成了和解。据 SEC 称，Pearson 公司同意支付 100 万美元的民事罚款，以

解决“不承认或否认调查结果”的指控，该指控试图掩盖和淡化 2018 年发生的数据泄露事件，此次泄露事件导致美国 1.3 万所学校的学生和管理员登陆凭证信息泄露。

https://www.freebuf.com/news/285017.html