全球数据安全观察

总第 106 期 2022 年第 34 期

(2022.09.12-2022.09.18)

大数据协同安全技术国家工程研究中心

NERCBDS
大数据协同安全技术
国家工程研究中心

目录

政策形势

1、国家网信办发布《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》

为了做好网络安全法与相关法律的衔接协调，完善法律责任制度，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益，国家网信办会同相关部门起草了《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》于14日公布。

本次拟从以下四个方面作出修改：一是完善违反网络运行安全一般规定的法律责任制度；二是修改关键信息基础设施安全保护的法律责任制度；三是调整网络信息安全法律责任制度；四是修改个人信息保护法律责任制度。

http://www.gov.cn/xinwen/2022-09/14/content_5709807.htm

2、国家标准《信息安全技术 网络数据分类分级要求（征求意见稿）》发布

9月14日，全国信息安全标准化技术委员会归口的国家标准《信息安全技术 网络数据分类分级要求》征求意见稿发布。

征求意见稿对数据分类框架和方法、数据分级框架、数

据分级确定方法、数据分类分级实施流程等内容提出要求。

https://www.tc260.org.cn/front/postDetail.html?id=20220914181019

3、《上海市公共数据开放实施细则（征求意见稿）》发布

为贯彻落实《上海市数据条例》《上海市公共数据开放暂行办法》等有关法律法规，上海市经济和信息化委员会发布《上海市公共数据开放实施细则（征求意见稿）》。

征求意见稿从数据开放、数据获取、开放平台、数据利用等方面提出公共数据开放要求。

https://app.sheitc.sh.gov.cn/gg/693375.htm

4、苏州市大数据集团有限公司、苏州大数据交易所正式揭牌

9 月 16 日，苏州市大数据集团有限公司、苏州大数据交易所正式揭牌，标志着数字苏州建设进入新阶段。

其中，苏州大数据交易所以建设全国一流的数据流通交易基础设施为目标，打造基于统一的可信计算能力底座，依托苏州市公共数据开放平台、苏州大数据交易平台两大平台，支持数字金融、数字制造、数字文旅等 N 个应用创新的“1+2+N”运营模式，不断整合公共数据、社会数据、算法算力等多方资源，打造具有苏州特色的数据资源化、资产化、价

值化商业模式，推进数字经济与实体经济有机融合。

https://www.suzhou.gov.cn/szsrmzf/szyw/202209/6ad9345b86864eea87cba8b2064e3f20.shtml

5、拜登签署新行政令：涉及芯片、AI、量子计算等领域

当地时间 9 月 15 日，美国总统拜登签署一项行政命令，，要求美国外国投资委员会（CFIUS）确保美国对不断变化的国家安全风险进行强有力的审查。

该行政命令详细阐述并扩展了美国外国投资委员会在审查国家安全风险交易时考虑的现有因素清单，并描述了关键领域潜在的国家安全影响。

其中两个法定因素包括：特定交易可能对事关美国国家安全的供应链产生影响，包括在国防产业之外的交易；特定交易会影响到美国国家安全领域的技术领先地位。

另外三个因素包括：特定交易可能影响事关美国国家安全的行业投资趋势；威胁事关国家安全的网络安全风险；事关美国人敏感数据的相关风险。

https://mp.weixin.qq.com/s/8AjGO8yzfywvtHhu4qSf3w

6、欧盟立法：数字产品必须遵守安全基线，违反者可罚全球收入 2.5%

9 月 16 日消息，欧洲公布了最新的网络安全基本要求提案《网络弹性法案》，要求**数字设备与软件开发厂商证明产品能够满足要求**，从而降低家用电器、可穿戴设备、软件与计算机等一系列产品遭黑客攻击的风险。

这项立法草案还要求，**在欧盟开展业务的制造商在产品生命周期内或投放市场后的五年内**（以较短者为准），**需持续提供安全补丁与更新**。违反规定的企业将面临最高 **1500 万欧元**（约 1.05 亿元人民币）或**全球营收 2.5%的罚款**。

https://www.secrss.com/articles/47012

技术、产品与市场

1、IDC: 2022 上半年中国 IT 安全硬件市场规模同比下降 2%

IDC《2022 年第二季度中国 IT 安全硬件市场跟踪报告》显示，2022 年第二季度中国 IT 安全硬件市场厂商整体收入约为 6.9 亿美元(约合 45.6 亿元人民币), 规模同比下降 12%。综合上半年数据，2022 上半年中国 IT 安全硬件市场规模达到 12.3 亿美元，同比下降 2%。

总体来看，2022 上半年中国网络安全硬件市场数据表现如下:

- 基于 UTM 平台的防火墙市场规模仍为最大，2022 上半年市场规模近 4.2 亿美金;
- 受到经济形势羸弱的影响，统一威胁管理硬件产品（UTM）2022 上半年市场规模同比降幅最高，达到 3.6%，增长压力逐步增大;
- 新常态下，虚拟专用网成为 2022 上半年唯一实现正增长的子市场，同比增长达到 8.7%;
- 从行业来看，政府、金融、运营商仍为三大主力投资行业，公共事业、能源、制造等行业在关基条例进一步落地的推动下增速喜人。
- 从省市地区来看，北部、东部、南部仍主导，但由于

上半年疫情等影响，上海等地区上半年的安全投入有所下滑。

https://www.secrss.com/articles/46888

2、[调研]三分之一的企业未加密云端敏感数据

Orca 最新公共云安全报告指出，大多数企业虽将云安全列为自身 IT 首要工作重点，却一直忽视了云端数据的基本安全措施。报告揭示，36%的企业在其云端资产中混有未加密的敏感数据，如公司秘密和个人身份信息等。

Gartner 预测，今年花在全球公共云计算服务上的支出会增长 20.4%，达到 4947 亿美元，并预计 2023 年将达到近 6000 亿美元。

公司最有价值的资产包括个人身份信息、客户及潜在客户数据库、员工和人力资源信息、企业财务信息、知识产权，以及生产服务器。公司需采用最高安全标准保护此类资产，并在决定哪些风险需首先缓解时将之排在最高优先级。

大约 36%的企业在文件、存储桶、容器和无服务器环境中存放有秘密和个人身份信息等敏感数据。 报告称：“加密可大大降低敏感数据遭无意暴露的可能性，而且只要不被破解，就能消除数据泄露的影响。”

https://mp.weixin.qq.com/s/H0TXeFBm5JgzzyUl9oBIKA

3、将隐私计算技术和区块链结合，首次试水建立风险数据共享平台

在中国资本市场金融科技创新北京首批试点中，中国证券业协会（即“中证协”）推出的“基于区块链和隐私保护技术的行业风险数据共享平台项目”，率先对该技术在金融领域的发展进行了探索和研究。

中证协刚刚对外发布“证券业联盟链”（简称“证联链”），为推进科技监管能力建设，促进证券业数字化转型提供行业新型基础设施。在行业联盟链上建立起风险数据共享平台，为首次尝试。具体来看，中证协将隐私计算技术和区块链结合，通过实现隐私数据可用不可见，隐私数据不出域达到数据共享。项目平台上共享的风险数据为证券公司开展相关信用业务提供参考，为风险评估提供帮助。

https://mp.weixin.qq.com/s/MDh3OFAy6DBJftZwVpBsfQ

4、国内首个自动驾驶数据分类分级白皮书

9 月 18 日，《北京市高级别自动驾驶测试示范区数据分类分级白皮书》于 2022 世界智能网联汽车大会网络与数据安全峰会正式发布，填补了国内自动驾驶示范区数据分级分类领域的空白，为行业数据安全管理提供“北京经验”。

白皮书以不同类型的示范区数据在遭泄露、破坏或非法

利用后带来的负面影响作为判断依据，从影响对象和影响程度两方面综合考虑，确定示范区数据的重要性等级。通过判断数据一旦遭到破坏、泄露、损毁等，对国家安全、公众利益、个人权益和企业合法权益的危害程度与影响，将数据等级分为 DL1-DL5 五个等级。

https://mp.weixin.qq.com/s/oSbtQUFbzqeXq-ELweZXEg

5、研究报告：十分之一的员工每 6 个月就可能泄露公司敏感数据

内部威胁是企业安全团队需要应对的持续威胁。这是一个全球性问题，但在美国尤为严重——2021 年有 4700 万美国人辞职，存在前雇员将敏感信息带给竞争对手、将其出售给犯罪分子以换取现金以及向媒体泄露文件的威胁，数据外泄日益受到关注。

网络安全公司 Cyberhaven 跟踪了全球约 140 万在其组织中处理敏感信息的人，以了解何时、如何以及谁参与了数据泄露。Cyberhaven 在其报告中指出，平均 2.5% 的员工在一个月内就会泄露敏感信息，但在六个月的时间里，将近十分之一的员工或 9.4% 的员工这样做了。当数据以未经批准的方式传输到组织外部时，就会发生数据泄露事件。

https://www.csoonline.com/article/3673260/one-in-10-

employees-leaks-sensitive-company-data-every-6-months-report.html#tk.rss_all?&web_view=true

业界观点

1、叶红：数据安全是网络空间安全基础，保护工作尚处起步阶段

中国信息协会信息安全专业委员会(下称“信安委”)主任叶红近日在接受中新财经等媒体采访时表示，数据安全的重要性越发凸显：“我们可以这样理解，数据是网络空间中的血脉，是其核心的要素，所以数据安全是网络空间安全的基础。”

叶红认为，在数字经济浪潮中，数据已成为一种新的生产要素，其价值和重要性直接关系到国家安全、社会稳定、企业生产经营及百姓日常生活，因此数据安全是数字经济长期稳定发展的重要保障。

她表示，从实际情况来看，不管是从法律意识上，还是工作行为及技术手段上，在整个社会层面，包括各个应用单位、厂商等对数据安全保护，应该说仍是刚刚起步，还有一些不足之处。

数据安全保护未来如何加强？叶红给出了三点建议：

其一是要**普及和加强数据安全法律意识和数据保护能**

力培养，使得各方意识到不论是政府、企业还是个人都要遵守相关法律要求。

其二是要**加紧落实数据安全法的配套措施**，例如数据分类分级问题，需要政府能及时出台一些操作指南给予指导。

其三是要**鼓励科研机构和企业加快研制数据安全保护的技术产品**，特别要注重针对一些新技术新应用，比如人工智能、隐私计算等，来解决相应数据安全保护中碰到的难题。

https://www.chinanews.com.cn/cj/2022/09-14/9852140.shtml

2、钟振山：隐私计算是数据安全领域增速最快的赛道，当下国内对零信任理解存在误区

根据 IDC 统计，2021 年中国数据安全产品与服务的总市场规模（包含隐私计算与区块链技术中的数据安全部分）达到 12.43 亿美金，约合 80.2 亿人民币。

“隐私计算可能是未来大家值得关注的领域。我国近几年发布了不少数据保护相关的法律，让数据使用更为规范和有据可循。随着数据安全被上升至法律层面，企业责任变得越来越大。而隐私计算的技术，在很大的程度上让企业降低个人信息泄露的风险。根据我们的预测，未来五年隐私计算在众多数据安全技术中，将是增速最快的一个市场。”钟振山说。

除了隐私计算外，零信任也是近年来较为热门的网络安全防护概念。钟振山透露，当下国内对零信任概念的理解存在一定的误区。

“很多企业把统一身份管理项目，也称之为零信任项目，但其实概念完全不同。身份管理是非常基础的能力，只有具备足够强的身份管理能力后，企业才有可能建设零信任安全体系，然而这并不等同于零信任。”

钟振山坦言，在调研过程中，很多厂商会自称提供零信任解决方案，但实际是 SSO (单点登录）这样的身份管理项目，“他们并不具备零信任所需要的整体技术能力。”

https://www.eet-china.com/mp/a160991.html

3、王建冬：数据要素市场化配置水平仍待提升

随着我国数据要素相关政策环境不断完善，相关法律规制逐步健全，数据要素资源规模持续扩大，数据交易市场日趋繁荣。

王建冬在分析了我国数据要素市场化配置水平、数据交易 2.0 时代总体特点等方面后，认为未来将形成以数据要素基础支撑体系为底座的多层级、立体化的数据交易市场体系和数据交易服务生态体系。同时，他从多方面发力构建全国统一的数据要素市场体系提出以下建议：

在**加强基础设施和标准规范建设**方面，他进一步建议称，可侧重统筹考虑数据交易场所、公共资源交易平台、算力资源体系等平台设施的互联互通机制，建立统一的数据流通标准和技术规范；鼓励交易机构、数据商、第三方服务机构、行业协会等探索完善数据采集、数据脱敏、数据质量、数据管理、数据价值评估等方面标准规范建设和贯标工作，打造高价值数据资源体系。

在**创新完善监管体制机制**方面，王建冬表示，可完善政府监管、平台监管与行业自律三位一体的多主体、跨部门的联合监管机制，加强数据流通行业相关执业标准和业务规范。加强数据反垄断和反不正当竞争执法，完善反数据垄断实施细则、程序和处罚相关规定。推动开展信用信息共享和合作，健全数据要素市场信用体系。

在**积极开展数据跨境流通试点示范工程**方面，则可推动跨境通信基础设施服务体系建设，探索开展跨境数据流通融合应用创新。探索建设深港“数据海关”监管机制，建立健全国际认可的数据跨境流通行政法规与标准体系。探索建设离岸数据交易平台，开展金融、科研、物流等重点行业数据跨境流通机制试点。

https://www.ndrc.gov.cn/wsdwhfz/202209/t20220913_1335479.html?code=&state=123

4、王文宇：数据安全不只是合规，亟需基于对抗的数据安全

6 月 22 日，西北工业大学发布《公开声明》称，该校遭受境外网络攻击，调查报告表明检测到超过 1100 条在内部渗透的攻击链路。数安行数据安全专家表示当前数据安全防护工作的难点主要包括两方面：一方面，在内部发生的各种数据访问、传输等合法的数据运营过程，会造成数据的大量复制、压缩、格式转换等等形态和数量上的变化，导致数据存储混乱、暴露面大、敏感数据无梳理，内部扩散滥用风险增大。另一方面，外部攻击窃密以网络钓鱼等手段攻破切入，盗取敏感数据外出时，也会提前进行多次的加密、隐写变形等等恶意伪装和掩饰处理，导致可以绕过边界处的审计、检测、拦截策略。

数安行王文宇认为，通过在 DataOps 中内嵌安全属性的方式，可以实现数据安全左移的技术落地。DataSecOps 是一种自动化的安全，基本思想就是在数据运营的第一现场持续地对数据处理和使用全流程进行追踪，这样才能监测到数据经变形处理流转的整个过程，直面数据的多态性和多副本性，发掘数据风险的真正源头，实现数据安全能力的延展。

https://www.sohu.com/a/585030641_120971648

5、专家：落实合规提升数据安全水平

近日，在2022（第八届）中国互联网法治大会——医疗健康数据安全合规论坛上，多位专家对落实合规提升数据安全水平提出建议。

工业和信息化部网络安全管理局数据安全处处长雷楠表示，医疗健康数据不仅是实现数字健康、医疗模式变革、效率变革、质量变革的关键纽带，也是数据安全保护工作的重点领域。建议从政策、联动、示范等三方面重点开展工作，加强核心技术产品公关，共筑风险防范的化解能力，营造全社会参与的良好氛围。

中国社科院法学研究所、国际法研究所联合党委书记陈国平表示，网络信息法是中国社科院的研究重点之一。目前，中国社科院与北京友谊医院共同设立医疗卫生与法治协同创新中心，开展医疗网络数据安全研究。现阶段，应进一步加强信息法治建设和医疗信息法治建设，各方携手研究做好医疗卫生数据安全合规工作。

中国信通院党委书记宋灵恩提到，中国信通院在医疗健康数据安全合规方面，开展了医疗健康网络数据安全自律、标准体系、课题研究等系列工作，将充分发挥中国信通院的专业技术优势和科研精神，全力支撑行业主管部门做好医疗健康数据安全合规工作，为实现健康中国 2030 目标贡献力

量。

中国工程院院士沈昌祥表示，医疗健康数据合规工作，相关部门高度重视、群众热切关注，建议从完善标准体系、开展合规培训、加强安全技能等方面，落实做好医疗健康数据安全合规，为医疗健康数字化转型保驾护航。

https://www.sohu.com/a/585762698_362042

数据安全事件

1、Google 和 Meta 因非法收集个人信息被韩国罚款千亿韩元

2022 年 9 月 14 日报道，Google 和 Meta 涉嫌在韩国未经用户同意收集个人信息并将此用于在线投放个性化广告，分别被罚 692 亿韩元和 308 亿韩元。韩个人信息保护委员会 14 日开会做出了上述决定。委员会还勒令两家公司若要收集和利用旗下用户利用其它公司平台的行为信息，必须提前通知用户，让用户容易、明确地了解情况并自由行使决定权。这是韩国就在线广告平台收集和利用用户信息的行为首次做出的处罚决定，罚款金额为违反《关于保护个人信息的法律》规定的案件之最。

https://www.solidot.org/story?sid=72762

2、Ambry Genetics 健康数据泄露诉讼达成 1225 万美元和解协议

2022 年 9 月 14 日，据外媒报道，Ambry Genetics 已与 232,772 名受其电子邮件系统在 2020 年 1 月遭到为期两天黑客攻击影响的患者达成了 1225 万美元的和解。诉讼称，该事件是临床基因组诊断供应商网络安全协议不足的“直接结果”。

该诉讼源于供应商于 2020 年 4 月首次报告的电子邮件事件，攻击者在该事件中获得了对单个员工电子邮件帐户的访问权限。该帐户包含患者姓名、医疗信息、诊断以及 Ambry 提供的服务的详细信息，一小部分患者涉及社会安全号码。

https://www.scmagazine.com/analysis/email-security/12-25m-settlement-reached-in-ambry-genetics-health-data-breach-lawsuit?&web_view=true

3、OakBend 医疗中心遭到勒索软件攻击，攻击者声称窃取了数百万美国公民的个人数据

2022 年 9 月 12 日，据外媒报道，OakBend 医疗中心宣布受到重大勒索软件网络攻击，迫使该中心重建其整个 IT 基础设施。

攻击者于 9 月 1 日发起攻击，在他们部署了勒索软件后，医疗中心的 IT 团队立即使所有系统脱机，并将一切置于锁定模式。虽然医院没有确定袭击者的身份，但一个名为 Daixin Team 的组织联系了 DataBreaches 网站并声称对此事件负责。他们还声称已经提取了 3.5GB 的患者数据，并提供了一些样本来证明他们应对这次攻击负责。

https://www.bitdefender.com/blog/hotforsecurity/oakbend-medical-center-hit-with-ransomware-attackers-claim-to-have-stolen-personal-data-of-a-millions-us-citizens/?web_view=true

4、思科证实阎罗王勒索软件组织窃取了企业数据

勒索软件黑帮阎罗王（音 Yanluowang）声称从思科网络窃取了数以千计的文件，总容量 55GB，其中包括机密文件、技术图表和源代码。但阎罗王没有提供证据证明其说法，只是公布了一张访问思科开发系统的屏幕截图。思科证实，阎罗王勒索软件组织在今年五月的一次攻击中从企业网络窃取了部分数据，但否认有任何敏感数据被盗。思科称阎罗王盗取了一名雇员的 VPN 账号，访问了该雇员的 Box 文件夹，但在勒索软件尝试加密系统前攻击就被阻止了。

https://www.solidot.org/story?sid=72740

5、阿根廷的布宜诺斯艾利斯市议会称其遭到勒索攻击

9 月 13 日报道，阿根廷首都的布宜诺斯艾利斯市议会称其遭到勒索攻击。该机构在几条推文中表示，攻击开始于上周日，其内部操作系统被攻击，WiFi 连接中断。机构称他们迅速采取了必要措施以确保工作的连续性，计划在周二恢复 WiFi 网络，并逐步启用其它的系统。截至美国东部时间周二下午，该机构的网站仍处于关闭状态，目前没有勒索团伙对此事负责。此外，阿根廷科尔多瓦司法机构在上个月也曾遭到勒索攻击。

https://therecord.media/buenos-aires-legislature-announces-ransomware-attack/

6、U-Haul 披露暴露客户驾驶执照的数据泄露事件

2022 年 9 月 12 日，移动和存储巨头 U-Haul International (U-Haul) 在客户合同搜索工具被黑客入侵以访问客户姓名和驾驶执照信息后披露了数据泄露事件。

在发现违规行为后于 7 月 12 日开始进行事件调查后，该公司于 8 月 1 日发现攻击者在 2021 年 11 月 5 日至 2022 年 4 月 5 日期间访问了一些客户的租赁合同。

https://www.databreaches.net/customer-data-from-hundreds-of-indonesian-and-malaysian-restaurants-hacked-by-desorden/

7、Rockstar Games 遭黑客攻击后泄露了 GTA 6 源代码和视频

9 月 18 日，据称，一名黑客入侵了 Rockstar Game 的 Slack 服务器和 Confluence wiki，侠盗猎车手 6 游戏视频和源代码被泄露。

这些视频和源代码 17 日首次在 GTAForums 上泄露，一个名为“teapotuberhacker”的威胁参与者分享了一个指向包含 90 个被盗视频的 RAR 存档的链接。威胁参与者表示，他们正在接受超过 10,000 美元的 GTA V 源代码和资产报价，但目前不出售 GTA 6 源代码。

https://www.bleepingcomputer.com/news/security/gta-6-source-code-and-videos-leaked-after-rockstar-games-hack/

8、美国海关复制大量公民私人信息

据《华盛顿邮报》当地时间 9 月 15 日报道，美国海关和边境保护局（CBP）的负责人在今年夏天的一次简报会上告诉国会工作人员，美国政府官员每年在机场、海港和边境口岸旅客手中查获多达约 1 万台电子设备，并从中拷贝数据至一个庞大的数据库。

据报道，约 2700 名海关和边境保护局官员无需通行证即可访问该数据库，且数据库正在迅速扩大，数据包含旅客

手机和电脑等设备中的照片、联系人、通话记录和信息等。
https://www.secrss.com/articles/46963

9、网络钓鱼者瞄准 Facebook 用户，窃取敏感信息

2022 年 9 月 14 日，据外媒报道，网络钓鱼者正在寻求用来自社交网络的虚假通知来欺骗 Facebook 页面的所有者，以试图让他们分享敏感信息。

他们用来收集用户信息的方法非常聪明: 他们通过 Meta Ads Manager 创建一个潜在客户生成表单，并将指向它的链接包含在网络钓鱼电子邮件中。这样的链接降低了电子邮件被标记为潜在恶意的可能性，并且还给潜在受害者带来虚假的安全感，因为电子邮件表面上能够显示来自的是 Facebook 并包含指向 Facebook 上托管页面的链接。
https://www.helpnetsecurity.com/2022/09/14/phishers-facebook/

10、星巴克新加坡称客户数据库遭到破坏

2022 年 9 月 18 日，据外媒报道，星巴克新加坡表示其客户数据库在网上遭受破坏，有 200,000 人的信息被盗。被盗数据包括姓名、性别、出生日期、电话、家庭住址等详细信息，并在一个在线论坛上出售，其中一个数据库的副本已经以 3500 新加坡币的价格出售。然而，该公司表示，由于它

不存储信用卡详细信息，因此没有采取任何信用卡详细信息。

https://tech.hindustantimes.com/tech/news/starbucks-singapore-says-customer-database-breached-716634197844 62.html