全球数据安全观察

总第 104 期 2022 年第 32 期

(2022.08.29-2022.09.04)

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《数据出境安全评估申报指南（第一版）》

9 月 2 日，为了指导和帮助数据处理者规范、有序申报数据出境安全评估，国家互联网信息办公室编制了《数据出境安全评估申报指南（第一版）》，对数据出境安全评估申报方式、申报流程、申报材料等具体要求作出了说明。

https://dsj.guizhou.gov.cn/xwzx/gnyw/202209/t20220902_76344969.html

2、中央网信办等四部门关于印发《数字乡村标准体系建设指南》

为深入贯彻落实习近平总书记关于乡村振兴的重要指示批示精神，认真落实《中共中央 国务院关于做好 2022 年全面推进乡村振兴重点工作的意见》《国家标准化发展纲要》《数字乡村发展战略纲要》部署要求，加快推动数字乡村标准化建设，中央网信办、农业农村部、工业和信息化部、市场监管总局会同有关部门制定了《数字乡村标准体系建设指南》。

《指南》中对数字乡村标准体系建设的总体要求、基本框架、建设内容、建设路径、组织保障等提出要求，并明确

了可参考的国家标准、行业标准；同时在数据安全标准部分强调主要包括数据分类分级、重要数据安全、应用与服务数据安全、数据处理活动安全、个人信息保护等标准。

http://www.gov.cn/xinwen/2022-09/04/content_5708228.htm

3、江苏省互联网信息办公室发布《江苏省数据出境安全评估申报工作指引（第一版）》

9 月 1 日，江苏省互联网信息办公室发布了《江苏省数据出境安全评估申报工作指引（第一版）》，对数据出境安全评估涉及的有关用于、适用范围、申报方式、申报流程、联系方式等事项进行说明。

https://jsnews.jschina.com.cn/yuanchuang/202209/W020220902583092858179.pdf

4、国家卫健委等三部门制定《医疗卫生机构网络安全管理办法》

近日，为指导医疗卫生机构加强网络安全管理，国家卫生健康委、国家中医药局、国家疾控局制定了《医疗卫生机构网络安全管理办法》。

其中在第三章明确了数据安全管理要求，包括建立数据安全管理组织架构、每年对数据资产进行全面梳理、建立健

全数据安全管理制度、操作规程及技术规范，以及建立健全数据安全管理制度、操作规程及技术规范等内容。

http://www.cctmis.org/zcfg/zc/1328.html

5、广东省工业和信息化厅关于印发《广东省企业首席数据官建设指南》

为建设数据管理高端人才队伍，充分挖掘数据资源价值，促进企业数字化转型，推动广东省数字经济高质量发展，广东省工业和信息化厅印发《广东省企业首席数据官建设指南》，对数据安全官的建设原则、建设内容、保障措施、等内容进行规范化指导，并对数据官的岗位设置、岗位能力素质要求、岗位职责等事项进行明确。

http://gdii.gd.gov.cn/gkmlpt/content/4/4001/post_4001126.html#2896

6、浙江搭建数据共享平台 医学检查检验结果全省互认

近日，国务院第九次大督查第六督查组在浙江省调研发现，浙江搭建检查检验数据互通互认平台，实现全省范围内医学检查检验结果互认共享，有效解决患者“重复检查”“多头检查”问题，缩短患者就医时间，减轻医疗费用负担。

为解决全省各地信息化水平存在差异问题，浙江加快推

进“健康云”项目，通过系统升级改造，优化传输速度，统一接入口径，强化数据审核管理。

http://www.gov.cn/hudong/2022-09/02/content_5708102.htm

技术、产品与市场

1、上海数交所首发面向全国的一体化数据流通智能系统技术框架

近日，上海数据交易所**首发面向全国的“一体化数据流通智能系统”技术框架。**该技术框架是为促进全国跨领域、跨地区、跨主体数据要素融合应用，构建安全高效的“国家级+省市级+行业级”的多层次数据要素市场体系，依托上海数据交易所自有云及链基础设施，实现覆盖全流程、全业务的智能化数据要素流通技术解决方案。

目前，各地数据要素流通平台建设正处于探索发展阶段。去年 11 月 25 日，上海数据交易所首发全数字化数据交易系统，初步实现了数据交易全时挂牌、全域交易、全程可溯。在此基础上，本次升级发布的技术框架实现了数据交易的多层次、全流程、全业务、一体化和智能化。

该技术框架由**核心业务系统**与**基础设施**两部分组成。其中，核心业务系统部分包括了**全国数据资产登记系统**与**niDts新一代智能数据交易系统**；基础设施部分包含了**上海数据交易所专有云**及**上海数据交易所资产链**。

https://mp.weixin.qq.com/s/L9mLgtp3O0fN88O_3uGqBw

2、2023 年企业网络安全预算热点与趋势，减少安全意识培训预算得不偿失

2023 年，企业的网络安全支出可能无法阻止衰退，但却可以帮助企业在衰退中脱颖而出。话虽如此，网络安全决策者们仍然面临着巨大压力，因为管理层要求他们优先考虑能够产生最大收益的安全技术。报告指出，2023 年企业网络安全预算支出有以下三大趋势值得关注:

（1）公司在云安全上的支出不足，在本地安全上的支出过多

报告指出，企业往往在云安全方面投入不足。虽然很多安全团队已经在云安全上花费了大量资金，但是鉴于未来两年 58%的组织将其应用程序组合迁移到公共云，因此云安全是一个需要持续增加投入的领域。

（2）支出转向托管安全服务提供商

Forrester 预测，迁移到云不会减少组织在服务上的支出，但托管安全服务的竞争加剧为企业提供了更多更好的选择。企业在传统托管安全服务提供商（MSSP）的支出将转向那些能够提供更好结果的新产品和新提供商。

（3）从长远来看，减少安全意识培训预算得不偿失

预算制定者削减安全开支的常见领域是安全意识和其他类型的安全技能培训。当经济形势不佳时，削减这些领域

的支出似乎很诱人，但与其他安全性支出相比，消减安全意识培训预算不会节省太多，反而会加剧技能短缺，并导致依赖远程办公的企业快速丧失安全性能力。

“人员依然是网络攻击的最大漏洞之一，”报告指出：“任何有助于提高员工的警惕性和复原力的投入都会使你受益。企业可能被误导的地方是，安全意识培训就是制作一个用户每年观看一次的 30 分钟视频。这不是有效的安全意识培训方法，安全意识和行为必须持续融入企业文化才能真正发挥效力。”

https://mp.weixin.qq.com/s/WZer-QvRcqYqnxRTngon-A

3、三分之一的组织不知道他们的公共云数据是否被泄露

Laminar 数据安全研究团队发布了其 2022 年安全专业洞察调查的结果。65.1% 的受访者表示他们目前将数据驻留在公共云（亚马逊网络服务、微软 Azure 或谷歌云平台）中。虽然公有云采用的复合年增长率接近 26%，但令人惊讶的是，受访者尚未加强这些资产的数据安全性。40.3% 的受访者表示他们使用公共云数据安全工具来监控内部和外部威胁以及数据泄露。

因此，许多组织缺乏对未经授权的公共云数据访问的可见性。38.3% 的受访者不知道他们在过去六个月中是否有第

三方成功窃取了他们的公共云数据，而 9.6% 的人最近经历过暴露。同样，37.4% 的受访者无法判断内部员工是否意外访问了云中的敏感数据。由于组织缺乏可见性，数据泄露率可能比报告的要高得多。

https://www.helpnetsecurity.com/2022/08/31/1-in-3-organizations-dont-know-if-their-public-cloud-data-was-exfiltrated/?web_view=true

4、到 2023 年，全球勒索软件损失将超过 300 亿美元

总部位于瑞士的网络安全公司 Acronis 日前发布的年中网络威胁报告中报告称，2022 年前六个月近一半的违规行为涉及凭据被盗。

毫不奇怪，网络犯罪分子使用这些凭据的主要目标是发动勒索软件攻击，这“仍然是对包括政府组织在内的大中型企业的头号威胁”。为了提取这些凭据，攻击者主要使用网络钓鱼技术，在 2022 年上半年有 600 封恶意电子邮件活动在互联网上传播，其中 58% 的电子邮件是网络钓鱼尝试，28% 是恶意软件。

“勒索软件正在恶化，甚至比我们预期的还要严重，”这家瑞士公司警告说，并提到 Conti 和 Lapsus 勒索团伙是国际安全服务的主要目标，并预计到 2023 年全球勒索软件损失

将超过 300 亿美元。

https://www.infosecurity-magazine.com/news/ransomware-exceed-30bn-dollars-2023/?&web_view=true

5、《2022 十大风控技术趋势指南》重磅发布，隐私计算在列

近日，在 “2022 IDC 中国数字金融论坛”上，国际权威咨询机构 IDC 联合蚂蚁集团正式发布了《十大风控技术趋势指南》白皮书。这是风控行业技术创新的一次风向标，也意味着和黑灰产对抗中技术升级迫在眉睫。白皮书指出多方风控主要由区块链及隐私计算技术支撑，比如可信执行环境（TEE），多方安全计算和联邦学习，能使得不同的机构能够在数据隐私得到极好保护的前提下进行风险数据共享，甚至联合建模。因此，为应对连通性风险，各商家、银行和第三方支付机构之间的“互联互通”十分必要，同时，还须保证这种“互联互通”的安全性。

https://mp.weixin.qq.com/s/5fFxY-yMxDVU7kxoY0fTBw

业界观点

1、360 钟力：安全是数字时代的底座 是一切正常运转的基础

9 月 1 日，2022 中国智能产业论坛在北京首钢园举行，本次论坛为 2022 中国国际服务贸易交易会的组成活动之一，主题为“数智时代 智创未来”。360 集团大数据协同安全技术国家工程研究中心副主任钟力博士出席并发言。

钟力博士表示，万物皆可云，安全也不例外。网络安全能力和数据安全能力都能够以云化的方式提供给用户。在数字化转型的过程中，企业都会面临着攻击面急剧扩大的问题，与此同时自身的安全资源投入却跟不上脚步，这就会带来一系列的安全问题。前不久 360 天枢智库发布的《中小微企业数字安全报告》显示，超过九成（92.3%）的中小微企业长期被黑客攻击而不能独立应对数字安全威胁，超八成（81.6%）的勒索攻击针对的是 1000 人以下的中小微企业。解决这些企业安全问题最好的方式，就是通过安全云比如 360 企业安全云来直接获得国内顶级的云化的安全能力和服务。

5G 让我们进入数字时代，钟力博士讲到了三个词：万物互联是其中一个，越来越多的事物将来甚至是所有的事物都将连接到互联网上；前面还有一个叫软件定义，智能化的设

备里面都会有软件，有软件就会有漏洞，有漏洞就可能会被利用而出现安全问题；第三个是数据驱动，现在数据驱动一切，从最早的电子商务到现在的数字城市、数字政府，各行各业都在数字化。可见，现在的一切都将会构建在数字技术之上，安全变得非常关键，成为一切正常运转的基础，需要为这个时代打造一个坚实的数字安全底座。基于安全大脑的数字安全能力体系就应运而生了，它以“看见”安全威胁、“处置”安全威胁为核心，通过大数据安全分析能力和积累了 16 年的 2EB 全球互联网安全大数据，加上 2000 余名顶级安全专家的运营，形成全球顶级的数字安全能力。目前，这样的一套能力体系正通过“数字安全基础设施+运营服务”的方式，复制到城市、行业、企业中，为我们这个世界的数字时代构建安全的未来。

https://finance.sina.com.cn/hy/hyjz/2022-09-01/doc-imizmscv8730948.shtml

2、朱萌：唯有安全可信，才能穿越技术周期

“以数据驱动的深度学习，其技术潜力已接近‘天花板’。”9 月 1 日，在 2022 世界人工智能大会-可信 AI 论坛，瑞莱智慧 RealAI 合伙人、高级副总裁朱萌发表了演讲。

朱萌指出，安全可信，已成为人工智能稳健发展的主要

抓手，也将逐步成为行业规范化、技术商业化的关键助推器。

“人工智能当前的安全风险主要可以从‘系统’与‘人’两个视角来剖析。”朱萌认为，系统层面来看，以深度学习算法为核心的人工智能系统十分脆弱，其结构性漏洞致使“对抗样本攻击”不可避免，而其数据依赖性则使其存在“数据投毒”漏洞，出现“后门攻击”。从“人”的层面来评估 AI 的可信问题，主要风险来自人的滥用、恶意应用，最为典型的就是深度合成技术。它大幅降低了信息生成合成的难度，但其负向应用已产生实质危害，甚至存在“武器化”风险。

https://www.sohu.com/a/581788835_121332532

3、刘杰：企业数字化关键内核：数据要素与算法应用

刘杰教授从管理学视角，对企业数字化的关键内核进行了高度凝练和系统阐释。在他看来，把握数字化需要理解两方面的本质问题，一是数据要素，二是算法应用。

刘杰认为，要应用好数据要素，有三个目标和四项任务。三个目标依次是**业务数据化、数据资产化和数据资产业务化**，比如贝壳将租房、买卖房业务数据化，并通过一些策略保障准确性。然后通过这些数据资产化，融资上市。有了更多数据资产，它就可以拓展更多的业务，比如装修等，形成杠杆效应。在这个过程中，企业有四项任务：一是**数据要素化**，

要让数据能流动起来充分应用；二是要**有数据思维**，比如企业管理不仅靠直觉、也要靠数据分析；三是要**有数据素养**，包括企业主和员工，能针对问题找数字技术解决，也能理解数字技术后找到新的应用价值；四是**把握数据生态**，今天的环境更需要有数据治理思维。

最后还要会用算法，包括数据收集、数据、算法、算力和应用（即“人”）五个要素的框架。有两方面主要任务，一是**业务算法化**，二是**算法业务化**。常规工作可以用算法取代，比如基于同类商品价格数据收集分析进行自动化定价。高端工作也可以用算法支持优化，比如战略决策算法化，亚马逊能基于大数据分析在世界各地进行仓库选址。

https://www.163.com/dy/article/HG604SVN0553SPG1.html

4、周延礼：建议保险行业建立统一平台，完善数据安全管理体系

“未来保险机构与监管部门应形成合力，完善数据安全管理体系，建立数据分级分类管理制度，明确保护政策，落实技术和管理措施。”8 月 27 日，全国政协委员、原中国保监会副主席周延礼在由新华网主办的“2022 第七届金融科技论坛”上表示。

具体来看，周延礼建议，一、要积极推进保险科技赋能，

提升科技硬实力；二、要建立统一的行业平台，推动数据互联互通；三、要加强网络安全保险，关注数据安全和隐私保护；四、要加强金融监管协调，提升监管科技综合水平。

http://m.caijing.com.cn/article/271742?target=blank

5、专家：卖手机前恢复出厂设置，个人信息仍会泄露

“恢复出厂设置和删除文件，并不等于彻底删除信息。”中国电子技术标准化研究院网安中心测评实验室副主任何延哲介绍，在手机上删文件，其实系统只是将该文件的指示路径删除，一般人找不到该文件了，但实质内容信息仍存储于手机内部。

何延哲说，目前恢复数据的技术门槛不高，恢复手机中以前的内容信息并非难事。从技术层面讲，即便用户先前做了一些简单的数据清除，删除的信息仍可恢复，可能只是需要多花一些时间和精力，个人信息泄露甚至被兜售的风险依然存在。

2011 年,《废弃电器电子产品回收处理管理条例》实施，废弃电子产品回收有了规范。但该《条例》并未对个人信息保护作出规定。“《条例》制定时，更多关注的是保护环境、促进资源综合利用和循环经济发展。”北京外国语大学法学院讲师李帅说，当时社会数字化程度还不高，电子产品中存储

的数据在体量和承载内容上与现在相比有较大差距，那时手机也没有如此强大的信息集成交互功能，对个人信息的保护不像当下紧迫。

李帅建议，将废弃电子产品回收列入信息保护范畴，提高个人信息泄露违法成本。同时，借鉴各地现有规定及实践，可先行制定规章层级的全国性法律规范，以废弃电子产品回收中的信息处理为主要规范对象，从基本原则、监管对象、监管方式与监管标准、违法责任等方面作出规定。“在监管上，应以数据安全法、个人信息保护法等为依据，厘清市场监管部门、工信部门等行政机关在信息保护监管中的职责，加大监管力度。”

有业内专家提醒，处理废弃电子产品最好通过正规大型店或平台，尽量避免小店和个人渠道。如今，各大手机厂商纷纷推出回收服务，承诺保证个人信息安全，有的厂商还会对数据清理过程全程录像监控。

https://www.sohu.com/a/580823697_120948862

数据安全事件

1、因未告知消费者出售其个人信息，丝芙兰被罚 120 万美元

近日，美国加利福尼亚州总检察长罗伯·邦塔（Rob Bonta）在发布会上表示，著名化妆品品牌丝芙兰（SEPHORA）就其侵犯消费者隐私一事与加州居民达成和解协议，决定支付 120 万美元的罚款，并在隐私政策中披露其向第三方出售消费者个人信息的事实，为消费者提供个人信息出售的退出机制。

https://www.secrss.com/articles/46381

2、BlackByte 勒索软件团伙窃取了 2 万人的信息

2022 年 9 月 2 日报道，全美橄榄球联盟的旧金山 49 人队正在邮寄通知信，确认在今年早些时候袭击其网络的勒索软件攻击后，属于 20,930 名受影响个人的个人信息（包括姓名和社会安全号码）被访问和/或被盗。

BlackByte 勒索软件团伙声称对此次事件负责，就在全美橄榄球联盟为 2022 年超级碗做准备之际，他们开始泄露据称从 49 人队网络窃取的文件。该勒索软件组织发布了一个档案，其中包含价值 292 MB 的文件，该团伙称这些文件是

从 49 人队受感染服务器上窃取的数据。

https://www.bleepingcomputer.com/news/security/san-francisco-49ers-blackbyte-ransomware-gang-stole-info-of-20k-people/?&web_view=true

3、黑山遭遇勒索软件攻击，黑客索要 1000 万美元

2022 年 9 月 1 日，Bleeping Computer 网站披露，黑山政府关键基础设施遭到了勒索软件攻击，黑客索要 1000 万美元巨款。

黑山公共管理部长马拉斯-杜卡伊在接受当地电视台采访时表示，此次网络攻击背后是一个有组织的网络犯罪集团，之后杜卡伊又补充说，黑客在这次攻击中使用了一种“特殊病毒”，并提出了 1000 万美元的赎金要求。

https://www.bleepingcomputer.com/news/security/montenegro-hit-by-ransomware-attack-hackers-demand-10-million/

4、图书馆业最大供应商遭勒索软件攻击：系统中断一周多仍未恢复

8 月 31 日消息，美国图书馆供应商 Baker & Taylor 公司日前披露，一周前曾遭到勒索软件攻击，目前仍在努力恢复各业务系统。该公司自称是全球最大的图书馆书籍和电子资

源分销商。

https://www.bleepingcomputer.com/news/security/leading-library-services-firm-baker-and-taylor-hit-by-ransomware/

5、国际移民政策制定中心遭到勒索团伙 Karakurt 的攻击

2022 年 8 月 31 报道，国际移民政策制定中心（ICMPD）遭到网络攻击导致数据泄露。ICMPD 在 90 个国家开展以移民为中心的研究、项目和活动。ICMPD 没有透露攻击发生的时间，但表示攻击者设法获得了对保存数据的单个服务器的有限的访问。该机构在检测攻击后的 45 分钟内成立了应急响应小组，断开了外部网络连接并关闭了所有网站。勒索团伙 Karakurt 在 Telegram 上称其对此事件负责，已窃取 375GB，涉及财务文件、银行数据和个人信息等。

https://therecord.media/migration-policy-org-confirms-cyberattack-after-extortion-group-touts-theft/

6、用友旗下畅捷通“中招”勒索病毒，企业用户被迫支付比特币“赎金”

2022 年 8 月 29 日，有用户在微博爆料称，用友旗下专注于小微企业云服务畅捷通 T+大面积出现勒索病毒。360 安全卫士和另一家厂商也报告确认了此次勒索病毒攻击。在安

全厂商与用户压力下，用友畅捷通在 29 日发布公告“回应”，承认有用户受到攻击。

《科创板日报》记者最新调查获悉，有用友畅捷通企业客户重要文件被勒索病毒加密，且用友方面也无法解密，被迫支付了 0.2 比特币（相当于 27439 元人民币）的“赎金”。

https://www.anquanke.com/post/id/279219

7、一个庞大的中国人脸和车牌数据库在网上泄露

2022 年 8 月 31 日，据 TechCrunch 报道，中国杭州一家科技公司新爱电子的面部图像和车牌数据库经历了一次大规模数据泄露。在高峰期，该数据库拥有超过 8 亿条记录，按规模计算，这是今年已知的最大数据安全漏洞之一。据称这是中国第二大数据泄露事件，该漏洞被认为可能是一次人为的错误。

https://www.databreaches.net/a-huge-chinese-database-of-faces-and-vehicle-license-plates-spilled-online/

8、泰国医学科学部系统遭黑客攻击，上万新冠患者数据被暗网售卖

据悉，网络犯罪分子从泰国医学科学部窃取了 PII 数据，这些数据包含有关新冠的信息。攻击者可能已经访问了至少

5,151 条详细记录，潜在暴露总数为 15,000 条。这些数据在几个暗网市场上出售，并可通过不良行为者创建的 Telegram 频道进一步购买。Resecurity, Inc.（美国）正在监控暗网中的数据泄露和数字身份数据的暴露情况，并已向执法部门和泰国 CERT 发出警报。

根据获得的样本和与安全事件相关的分析发现，不良行为者能够未经授权访问政府门户，从而非法管理用户和记录，并窃取敏感和个人信息，包括但不限于姓名、性别、年龄、联系方式、病史和相关的当地医疗保健标识。

https://www.secrss.com/articles/46397

9、美国国税局 (IRS) 错误地泄露了大约 120,000 名纳税人的机密信息

2022 年 9 月 2 日，美国国税局宣布意外泄露了纳税人的数据。财政部表示，这个问题是在 8 月 26 日发现的，但没有透露机密信息公开了多长时间。公开的数据包括这些纳税人的姓名、联系信息和报告的收入。社会安全号码、个人纳税申报表和其他敏感数据没有暴露。财政部已指示美国国税局迅速审查其做法，以确保采取必要的保护措施，防止未经授权的数据泄露。

https://securityaffairs.co/wordpress/135271/security/irs-data-

leak.html

10、俄罗斯流媒体巨头遭恶意攻击，210 万中国用户数据泄露

安全内参 8 月 30 日消息，俄罗斯流媒体巨头 START 某个 MongoDB 数据库暴露在公网，72GB 大小的 4400 万用户数据遭恶意黑客窃取，其中包括 210 万中国用户。泄露的信息包括用户名、电子邮件地址、哈希密码、IP 地址、用户注册国家、订阅起始及结束日期，以及最后一次登录记录。

https://www.secrss.com/articles/46367

11、Nelnet Servicing 被入侵后泄露 250 万个学生的贷款信息

2022 年 8 月 29 日报道，在黑客入侵技术服务提供商 Nelnet Servicing 的系统后，俄克拉荷马州学生贷款管理局(OSLA)和 EdFinancial 的学生贷款数据泄露。OSLA 和 EdFinancial 使用 Nelnet Servicing 的技术服务用于在线贷款的学生访问其贷款账户。攻击者在 6 月份入侵了 Nelnet Servicing，并一直存在到 7 月 22 日。据悉，攻击者可能是利用漏洞入侵了公司的网络，约 2501324 人受到影响。目前，EdFinancial 和 OSLA 都通过 Experian 为受影响的用户免费提供 24 个月的身份盗窃保护服务。

https://www.bleepingcomputer.com/news/security/nelnet-servicing-breach-exposes-data-of-25m-student-loan-accounts/

12、超过 1,800 个 Android 和 iOS 应用程序被发现泄露了硬编码的 AWS 凭证

2022 年 9 月 1 日报道,研究人员已经在 Android 和 iOS 上发现了 1,859 个包含硬编码 Amazon Web Services (AWS) 凭证的应用程序，这构成了重大的安全风险。

“超过四分之三 (77%) 的应用程序包含有效的 AWS 访问令牌，允许访问私有 AWS 云服务。”赛门铁克的研究人员表示。这些凭据通常用于下载应用程序功能所需的适当资源，以及访问配置文件和对其他云服务进行身份验证。这些令牌授予对云中所有私有文件和 Amazon Simple Storage Service (S3) 存储桶的完全访问权限。这包括基础设施文件和数据备份等。

https://thehackernews.com/2022/09/over-1800-android-and-ios-apps-found.html