全球数据安全观察

总第 117 期 2022 年第 45 期

（2022.12.05-2022.12.11）

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、《互联网信息服务深度合成管理规定》发布

11 月 25 日，国家互联网信息办公室、工业和信息化部、公安部联合发布《互联网信息服务深度合成管理规定》，自 2023 年 1 月 10 日起施行。规定对互联网信息服务深度合成技术与服务的一般规定、数据和技术管理规范、监督检查和法律责任等方面提出了明确要求。

http://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm

2、《最高人民法院关于规范和加强人工智能司法应用的意见》发布

12 月 9 日，最高人民法院发布《关于规范和加强人工智能司法应用的意见》，明确司法人工智能产品和服务需遵循安全合法、公平公正、辅助审判、透明可信、公序良俗五项原则，并提出要加强基础设施建设和安全运维保障，强化网络安全、数据安全和个人信息保护能力。

https://www.court.gov.cn/fabu-xiangqing-382461.html

3、六部门关于修改《网络预约出租汽车经营服务管理暂行办法》的决定

11 月 30 日，《关于修改〈网络预约出租汽车经营服务管理暂行办法〉的决定》经工业和信息化部、公安部、商务部、市场监管总局、国家网信办同意，予以公布，并自公布之日起施行。办法中明确了网约车平台公司、网约车车辆和驾驶员需遵循的数据安全、个人信息保护要求及责任。

http://www.gov.cn/zhengce/zhengceku/2022-12/05/content_5730599.htm

4、山东省关于组织开展山东省工业企业数据赋能专项行动的通知

12 月 6 日，山东省工业和信息化厅就组织开展工业企业数据赋能专项行动发布通知，提出推动企业数据全面采集、提升企业数据传输能力、创新企业数据存算模式、提高企业数据管理水平、深化企业数据融合应用五项重点任务，并明确强调要引导企业强化态势感知、测试评估、预警处置等数据安全能力建设，全面保障数据安全。

http://gxt.shandong.gov.cn/art/2022/12/6/art_15201_10320384.html

5、《四川银行业个人信息保护公约》发布

近日，四川银保监局指导四川省银行业协会发布《四川银行业个人信息保护公约》，适用于银行业金融机构对个人信息收集、存储、使用、加工、传输、提供、公开、删除等各个环节。公约共包括 4 个部分 12 条具体约定。

一是将个人信息保护纳入银行业金融机构业务经营和风险管理的全过程。建立健全个人信息的内部管理制度、操作规程。建立安全事件应急预案。

二是明确“五个不得”。不得向外出售、提供、泄露个人信息。不得未经许可在业务宣传、接受采访等活动中公开个人信息。不得非基于工作用途查询、复制、存储、使用个人信息。不得收集与业务或所提供服务无关的信息。不得采取不正当方式收集个人信息。

三是强化个人信息数据安全保护。建立数据安全制度体系，完善机制流程。保证存储介质及传输通道、节点和数据的安全，防控数据泄露、窃取、篡改、毁损等风险。

四是加强监督处置。银行业金融机构负责对其各级机构履行公约的情况进行监督检查。

四川省银行业协会对于违反公约致使行业形象受损的会员单位，按有关规定实施自律性处罚。对违法处理个人信息涉嫌犯罪的，及时移送公安机关依法处理。

https://mp.weixin.qq.com/s/dc-eOvaMyQw94W-9CLKGPg

6、9 项密码行业标准发布

11 月 20 日，国家密码管理局发布 9 项密码行业标准，自 2023 年 6 月 1 日起实施，包括:

1) GM/T 0117-2022 网络身份服务密码应用技术要求

2) GM/T 0118-2022 浏览器数字证书应用接口规范

3) GM/T 0119-2022 PLC 控制系统及 PLC 控制器密码应用技术规范

4) GM/T 0120-2022 基于云计算的电子签名服务技术实施指南

5) GM/T 0121-2022 密码卡检测规范

6) GM/T 0122-2022 区块链密码检测规范

7) GM/T 0123-2022 时间戳服务器密码检测规范

8) GM/T 0124-2022 安全间隔与信息交换产品密码检测规范

9) GM/T 0125.1-2022 JSON Web 密码应用语法规范 第 1 部分: 算法标识

10) GM/T 0125.2-2022 JSON Web 密码应用语法规范 第 2 部分: 数字签名

11) GM/T 0125.3-2022 JSON Web 密码应用语法规范 第 3 部分: 数据加密

12) GM/T 0125.4-2022　　JSON Web 密码应用语法规范 第 4 部分：密钥

https://www.oscca.gov.cn/sca/xwdt/2022-11/20/content_1060961.shtml

7、中国计算机行业协会数据安全专业委员会发布 4 项关于数据安全团体标准立项的通知

根据《中国计算机行业协会团体标准管理办法》相关规定，经立项评审，中国计算机行业协会批准《高性能可靠多方安全计算产品技术要求和测试评价方法》、《数据分类分级产品技术要求》、《邮件数据安全防护技术评价标准》、《平台生态数据安全基本要求》4 项团体标准立项。

https://mp.weixin.qq.com/s/hWfnAwB9AFZ0vWXG1qR1dQ

技术、产品与市场

1、超过半数 EDR 工具存在严重漏洞，数亿端点面临风险

安全产品（如 EDR 工具）往往拥有系统的超级用户权限，一旦被黑客入侵可用来发动几乎无法检测的攻击，造成难以估量的巨大损失。

在 12 月 7 日举行的欧洲黑帽大会上，SafeBreach 安全研究员 Yair 发表了主题为“开发下一代擦除器”的演讲，并公布了对多家安全厂商的 11 种 EDR 工具的测试结果，其中四家厂商的六种工具存在严重漏洞。这些易受攻击的产品分别是 Microsoft Windows Defender，Windows Defender for Endpoint、TrendMicro ApexOne、Avast Antivirus、AVG Antivirus 和 SentinelOne。

Yair 还在黑帽大会上发布了名为 Aikido 的概念验证代码（一个数据擦除器），演示了仅拥有非特权用户权限的擦除器如何操纵存在漏洞的 EDR 工具擦除系统上的几乎所有文件，包括系统文件。超过半数的受测 EDR 和 AV 产品中存在该漏洞，包括 Windows 上的默认端点保护产品。

https://www.secrss.com/articles/49827

2、ARR 超 2.5 亿美元，Recorded Future 成为全球最大威胁情报公司

2022 年 11 月 28 日，总部位于波士顿的威胁情报公司 Recorded Future 宣布其年度经常性收入(ARR)已超过 2.5 亿美元，成为全球最成功的 SaaS 公司行列。这标志着该公司的一个重要里程碑，并巩固了其作为不断增长的市场领导者的地位，证明情报对于抵御融合的威胁至关重要。

ARR（Annual Recurring Revenue）即年度经常性收入，是衡量 SaaS 企业经营优劣的基本指标，一般是指 SaaS 的订阅模式这部分收入。ARR 的特别之处在于收入的[经常性]，也就是说如果没有特别情况，这个收入明年会继续有（且数额也不会有太大的波动），因此 ARR 也经常被用作评判未来 SaaS 收入可衡量和可预测性的核心指标。

https://www.secrss.com/articles/49706

3、十大基于风险的漏洞管理工具

基于风险的漏洞管理工具为 IT 安全团队提供了一种持续的自动化能力，可以根据网络漏洞对特定组织构成的相对风险来识别、确定优先级和修复这些漏洞。

由于大型复杂互联计算环境中存在大量漏洞，企业难以及时部署所有软件补丁和补救措施，因此迫切需要具有机器

学习功能的自动化工具，以快速识别和上报在特定场景中风险最高的漏洞。领先的漏洞管理软件提供商正纷纷将基于风险的解决方案整合到产品中来满足这一需求。

Gartner 预计，到 2022 年基于风险的漏洞管理市场规模将达到 6.39 亿美元。其他分析公司估计，2022 年广义的漏洞管理市场规模已经超过了 20 亿美元大关。根据 IDC 的估计，2020 年基于设备的漏洞管理市场规模为 17 亿美元，年增长率为 16%，到 2022 年将达到约 22 亿美元。

据多个评测平台的排名得分和同行评测，VentureBeat 编制了一个基于风险的漏洞管理工具的 TOP10 榜单:

（1）Rapid7 InsightVM；（2）Arctic Wolf Managed Risk;（3）CrowdStrike Falcon Spotlight;（4）Tenable IO;（5）Qualys VMDR;（6）思科的 Kenna Security;（7）Frontline Vulnerability Manager;（8）Tanium;（9）微软;（10）Syxsense Enterprise。

https://www.wangan.com/p/11v6c0a1fd4192fc

4、2022 年暗网市场三大趋势

据《网络犯罪》预测，2023 年全球网络犯罪造成的损失将高达 8 万亿美元，网络犯罪市场将成为规模仅次于中国和美国的全球第三大“经济体”，其“GDP”增速更是高达 15%。暗网市场的繁荣得益于（导致数据泄露的）网络攻击的快速

增长。根据网络安全公司 SonicWall 最新公布的数据，2022 年网络攻击全面增长，各种技术和策略不断丰富，从入侵和恶意软件到较新的攻击媒介，如加密劫持和 NFT 犯罪。

以下是 2022 年值得关注的暗网市场三大新趋势:

（1）暗网市场爆发“价格战”。 2022 年暗网产品价格普遍下降，从恶意软件和拒绝服务攻击到加密货币交易所的失窃账户都不能幸免。

（2）六大热门暗网市场。2022 年规模最大的六个暗网市场（按市场份额百分比排序）:

- Dark0de：37%
- ToRReZ：30%
- DarkFox：21%
- ASAP：10%
- Cannazon：2%
- G.Dreams：不到 1%

（3）240 亿用户账户“上市流通”。 根据 DigitalShadows 发布的数据泄露报告“2022 年账户接管调查”, 2022 年总计超过 240 亿用户账户凭证在暗网论坛和犯罪市场中流通，这个数字比两年前暴增了 65%。

https://www.secrss.com/articles/48824

5、人工智能应用面临 7 大数据安全威胁

自动驾驶技术、智能助理、人脸识别、智能工厂、智慧城市等人工智能技术现已广泛落地，这些令人难以置信的技术正在快速改变我们的生活。但相关领域安全事件也在快速增加，这使得研究人员和使用者对人工智能的安全性担忧不断提高。人工智能应用带来的红利和其引发的安全隐患，犹如一个硬币的两面，需要全行业高度关注并找到有效的应对方法。

日前，安全研究人员梳理总结了目前人工智能技术在实践应用中经常要面对的 7 个数据安全威胁:

威胁 1：模型中毒

威胁 2：隐私泄露

威胁 3：数据篡改

威胁 4：内部威胁

威胁 5：针对性蓄意攻击

威胁 6：大规模采用

威胁 7：AI 驱动的攻击

https://mp.weixin.qq.com/s/xT7e_QrrjdKhjCNLEYGvZA

业界观点

1、专家：挖掘数据要素潜能

随着信息技术与经济社会的融合，数据成为驱动数字经济发展的引擎。如何促进数据要素的高效配置，怎样进一步激活数据要素潜能？日前在京举行的数据安全与数据要素化研讨会上，与会专家围绕这些问题展开了讨论。

在推动数据市场化改革方向和路径上，中国经济体制改革研究会会长彭森认为，要处理好政府与市场的关系，引导数据要素市场化配置，不断激发市场活力，同时也要处理好制度创新和技术创新的关系以及构建兼顾效率、公平、安全的数据治理体系。

中国电子信息产业集团副总经理陆志鹏结合实践分析认为，从目前信息技术发展的趋势看，数据资源和数据应用之间应进行解耦，即存在一个可被定义为“数据元件”的中间态。通过这种方式，将数据的所有权和使用权分开，明晰数据的权利归属；再把数据从资源到应用形成三级市场——数据资源、数据元件市场和数据产品市场，以此来解决定价、分配等问题，构建灵活高效的数据要素流通体系。

“数据只有流动起来，才能发挥它的作用，提高生产力。”清华大学社会科学学院经济学研究所副所长戎珂说。

近年来，国内企业在破解数据安全与数据要素化、市场化等难题方面，取得了一系列进展。中国电子数据治理工程指挥部技术部主任国丽举例说，为实现对整个数据要素化全流程的管控、调度和任务分配，他们率先研制出业界首个数据要素操作系统。

“作为链接数据要素化生态产业链的核心能力平台，数据要素操作系统向下可以对接各类数据工具、数据资源，向上可以对接各业务平台。下一步，我们将以此为基础，在更多地方探索制度、市场、技术相结合的落地实践，推动数据低成本、高效率的流通和交易。”国丽表示。

https://wlaq.gmw.cn/2022-12/05/content_36209454.htm

2、创新底层数字基础设施，助力老年群体数据安全

12 月 2 日，中国网络空间安全协会、伏羲智库共同在第十七届联合国互联网治理论坛上以“线上+线下”相结合方式主办了主题为“保障弱势群体的数字权利及数据安全——老年人的数据安全和个人信息保护的探索与实现”的研讨会。

清华大学互联网治理研究中心主任李晓东教授出席做主题发言并参与讨论，提出无论是年轻人还是老年人，面临的数据安全问题没有本质差别，不同的是老年人的安全保护意识更弱，更容易上当受骗导致数据被滥用。增强老年人的

安全意识固然重要，但核心还是要解决数据因流通利用而带来的安全风险问题。

目前国内外都在讨论数据的互操作性，其中很重要的内容就是在数据不出域的前提下实现数据的互联互通，实现数据价值的流动。在万物互联的时代，通过底层技术架构的革新来解决数据安全问题，在保护隐私的前提下释放数据价值，是未来数字技术适老化改造的一大趋势。

互联网发展的“下半场”，用户对自身数据的所有权意识和控制意愿都正在觉醒，破除数据圈占生态，赋予用户自主权成为发展的主流。在此背景下，数据与应用解耦将成为未来的发展趋势之一，实现数据的互操作性将成为数据生态的底层支撑和内生特性，以解决数据跨域互联、共享交换等联通问题，为数据生态的良性循环提供更多空间。

https://news.bjd.com.cn/2022/12/07/10256227.shtml

3、政企机构筑牢数据安全防线需要“三步走”

12 月 2 日，由贵州省委网信办主办的“强化网络安全保障体系 护航数字经济发展创新”论坛在贵阳市举行。奇安信集团董事长齐向东表示，数据强监管时代已经到来，政企机构应通过“盘清资产、精准防护、全局管控”的“三步走”，来破解数据安全防护难题，守好数据安全红线。

齐向东指出了当前数据安全防护面临的四大难题：一是数据资产梳理不清，被盗窃 100M 的数据和被盗窃 1 个 T 的数据概率相同，防线一旦被突破将导致“一失万无”；二是特权账号管理不严，管理员、技术员、操作员三员”安全隐患大；三是 API 接口管控不当，一点被突破，容易造成安全防线全面溃败；四是风险感知不全面，如遇到“蚂蚁搬家式”的盗窃手法，很难及时告警。

齐向东给出了数据安全系统治理的三大关键举措：盘清资产、精准防护、全局管控。

第一步，盘清资产。系统梳理业务系统、应用、数据等，并形成数据资产梳理报告。第二步，精准防护。一方面，要做好特权账号管理，做到能审查、能告警、能拦截；另一方面做好 API 管理，可通过 API 安全卫士及时发现 API 异常行为，提防外部攻击。第三步，全局管控。以“零信任”策略为核心，实现“权限最小化”，降低被攻击的风险；通过数据安全态势感知，对各类安全日志进行研判，快速响应处置。

http://www.ocn.com.cn/shangye/202212/cesjf05205910.shtml

4、重视数据合规，构建数据安全防线

“数据合规”就是围绕“数据”开展的合规工作，一般包括网络数据安全合规、个人信息保护合规、数据全生命周期合

规、数据安全审查及数据跨境等合规。公司信息建设运维中心在做好信息系统运行支撑的同时,大力开展数据合规性检查工作,主要分以下几个步骤:

第一步，摸清家底，主动梳理本中心的在运系统、APP等服务清单。

第二步，风险有数，按照数据合规评估项进行数据风险排查。

第三步，合理评估，组织数据合规评估团队进行数据合规性评估。

第四步，及时应对，积极开展数据合规风险整改，落实整改方案和动作。

第五步：定期审查，定期对数据合规措施进行审查，定期通报数据合规工作，建立相应的数据合规审查标准。

通过开展业务数据合规检查，一方面，确保企业所处理的数据以最小的丢失、被盗或滥用风险进行管理的过程，以实现对法律法规和相关标准的遵守；另一方面，也禁止企业在未经授权的情况下使用其他受保护的数据。

http://www.lzbs.com.cn/licai/2022-12/05/content_504344378.htm

5、我国数据要素流通的现状、困境与解决思路

数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通、消费和社会服务管理等各个环节，深刻改变着生产方式、生活方式和社会治理方式。

当前，我国数据要素流通现状特点主要包括我国数据要素政策布局逐渐细化、以公共数据为主要对象的数据开放共享持续推进、以数据交易所为主要载体的数据交易重掀热潮。

面临困境主要包括：合规尺度不明，流通预期不稳；相互缺信任，权益难保障；数据安全和隐私保护隐患重重。

面对数据要素流通的种种困境，需要营造审慎包容的市场环境，鼓励市场主体积极探索数据流通的解决方案与技术手段，在政产学研各界的协同发力中不断创新，促进数据要素的健康发展：推进制度体系建设，划定法律监管红线；充分发挥市场作用，开展数据流通试点；充分发挥市场作用，开展数据流通试点。

http://cbdio.com/BigData/2022-12/06/content_6171261.htm

数据安全事件

1、法国电力公司因 MD5 算法存储密码及数据收集问题遭监管罚款

法国数据保护监督机构于 11 月 29 日，对电力供应商法国电力公司（EDF）处以了 60 万欧元的罚款，因为它违反了欧盟通用数据保护条例（GDPR）的多个要求。做出处罚的依据是 GDPR 第 32 条规定：**数据控制者必须确保其实施的自动数据处理有足够的安全性，实现个人资料的假名化及加密。**法国电力公司（EDF）是一家法国能源巨头，拥有 840 亿欧元的营业额和近 2600 万的客户。

法国国家信息与自由委员会(CNIL)表示，罚款的一部分缘由是 2022 年 7 月**该公司使用 MD5 算法，对超过 25800 个账户的密码进行了散列处理，并储存了这些密码。**

https://www.secrss.com/articles/49824

2、法国巴黎又一医院因遭遇勒索攻击暂停运营并转移患者

12 月 5 日消息，上周末，法国巴黎一家综合性医院遭到勒索软件攻击，被迫叫停医疗手术并转移了 6 名患者。

法国卫生部表示，凡尔赛医院中心目前已经陷入无计算机系统可用的困境，该医疗综合体旗下有两所医院与一家养老院。

https://therecord.media/french-hospital-complex-suspends-operations-transfers-critical-patients-after-ransomware-attack/

3、城市管理软件供应商 Digipolis 服务器遭遇勒索软件攻击

安全内参 12 月 7 日消息，由于合作的数字供应商 Digipolis 日前遭受网络攻击，**西欧国家比利时的安特卫普市的数字服务被迫中断，目前正努力恢复**。造成服务中断的应该是勒索软件攻击，但幕后黑手是谁尚不明确。

服务中断影响到当地市民、学校、日托中心和警署所使用的服务。截至目前，各项服务仍处于时断时续的不稳定状态。

https://www.secrss.com/articles/49818

4、Hive 勒索组织黑五期间攻击欧洲零售商，已累计攻击 1300 家公司

近日，Hive 勒索软组织在其暗网泄露网站上发布了一批 Intersport 数据，并威胁说除非零售商支付勒索费，否则将泄露更多数据。据法国《世界报》报道，黑客攻击包括法国北部商店的 Intersport 员工的护照信息、工资单、其他商店的离职和在职员工名单，以及社会保险号码。黑客攻击发生在 "黑色星期五 "销售期间，使员工无法进入收银系统，迫使商店进行人工操作。

美国联邦政府在11月底表示，Hive已经袭击了全球1300多家公司，收取了约1亿美元的赎金。

https://www.freebuf.com/news/351975.html

5、新西兰多个政府机构的 MSP Mercury IT 遭到勒索攻击

据媒体12月7日称，托管服务提供商(MSP)Mercury IT遭到攻击，影响了该国的数十个公司和政府机构。司法部和新西兰卫生部透露因为此次攻击，他们的部分文件无法访问。卫生部还称现阶段这些文件并未受到未经授权的访问或下载，且卫生服务也没有中断。非营利性健康保险提供商BusinessNZ 也宣布其日常运营和客户服务受到影响。目前，新西兰相关部门正在开展紧急工作，以了解受影响的组织数量、所涉及信息的性质以及信息泄露程度。

https://therecord.media/multiple-government-departments-in-new-zealand-affected-by-ransomware-attack-on-it-provider/

6、云计算公司 Rackspace 确认遭勒索软件攻击

德克萨斯州的云计算提供商 Rackspace 已确认在被勒索软件攻击后被迫关闭其 Hosted Exchange 环境。Rackspace 托管的 Microsoft Exchange 服务于12月2日出现问题，6日，该公司确认导致中断的可疑活动是一起勒索软件攻击。目前，

该公司表示，正在为 Microsoft 365 上的数千名客户恢复电子邮件服务。
https://www.ithome.com.tw/news/154586

7、在线零售平台 Vevor 服务器配置错误泄露超过 1 亿条记录

据媒体 12 月 8 日透露，研究团队发现了一个无密码保护的数据库，其中数据集总大小为 601.84 GB，文档总数超过 1.16 亿。经调查，这些数据属于加利福尼亚的在线零售商 Vevor，一个专注于设备和工具的品牌。该服务器是在 2022 年 4 月首次被发现，然后研究人员在 2022 年 7 月再次发现不安全的 AWS 服务器，被托管在不同的 IP 地址上。2022 年 4 月的事件泄露了 406.79 GB 数据，包含 706206770 个文件；2022 年 7 月泄露了 601.84 GB 数据，1166293742 个文档。据悉，这是由于服务器所有者配置错误导致的。
https://www.websiteplanet.com/blog/vevor-breach-report/

8、以色列多家物流公司约 50 GB 个人和运输记录在暗网出售

据媒体 12 月 5 日报道，约 50 GB 的数据库在暗网上出售，数据发布时间为 2022 年 11 月 26 日和 27 日。调查显示，

这些数据属于 29 家以色列的运输、物流和货运公司。研究人员认为，黑客通过软件供应商的单点故障，未经授权进入这些物流公司的供应链，并窃取了大量个人数据和运输记录。每个数据库的售价为 1 BTC，相当于 17000 美元。攻击者总共列出了 110 万条记录，尚不清楚会影响多少人。

https://www.hackread.com/israel-logistics-employees-data/

9、MT Bangladesh 声称已入侵印度 CBHE 并窃取个人信息

媒体 12 月 5 日透露，名为 TeamMysteriousBangladesh（MTBangladesh）的团伙声称已入侵印度中央高等教育委员会(CBHE)的系统。该团伙表示窃取了 2004 年至 2022 年的学生信息，并发布了样本。CloudSEK 解释说，访问 CBHEDelhi 平台管理面板的任何人都可以查看 2004 年至 2022 年所有学生的成绩，甚至可以删除或添加。因此，攻击者可能获得了管理面板的访问权限，然后破坏了 CBHE 的数据。

https://cloudsek.com/threatintelligence/indian-central-board-of-higher-education-compromised-by-team-mysterious-bangladesh/

10、多个团伙利用社保公积金系统漏洞，非法获取公民个人信息 2300 万条

12 月 7 日，红星新闻从四川南充市公安局顺庆区分局获悉，当地警方侦破一起公安部挂牌督办案件，打掉多个利用社保、公积金等系统漏洞非法获取公民个人信息的犯罪团伙，涉及四川、河南、广东多个省市，抓获犯罪嫌疑人 121 人，查获公民个人信息 2300 余万条，发现国内多地各类信息系统平台漏洞 300 余个，收缴黑客工具 12 套。

2022 年 4 月，南充市公安局顺庆区分局网安大队民警在工作中发现，男子杨某利用境外聊天软件（Telegram）贩卖某市社保查询信息系统漏洞及侵入教程。通过这些漏洞和教程，犯罪分子能轻松绕过系统安全保护，通过链路授权访问省级社保系统，进而非法获取省级社保系统用户的全量数据。

https://www.secrss.com/articles/49866

《全球数据安全观察》周报

政策形势： 政策法规/地方动态/标准动态

技术、产品与市场： 技术研究/行业洞察/市场趋势

业界观点： 大咖观点/业界报告

数据安全事件： 合规事件/数据泄露/数据勒索

编委会： 唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nercbds@163.com

http://www.nelab-bdst.org.cn/