全球数据安全观察

总第 114 期 2022 年第 42 期

(2022.11.14-2022.11.20)

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、国务院关于数字经济发展情况的报告

11 月 14 日，于 10 月 28 日在第十三届全国人民代表大会常务委员会第三十七次会议上审议的《国务院关于数字经济发展情况的报告》发布。

报告在当前面临的总体形势中明确指出要“全面加强网络安全和数据安全保护，筑牢数字安全屏障”，包括贯彻落实网络安全、数据安全相关法律法规与制度要求，建立健全数据安全治理体系，加强数据跨境流动安全管理，推动数据安全产业发展，加强个人信息保护，提升数据安全保证水平。

http://www.npc.gov.cn/npc/c30834/202211/dd847f6232c94c73a8b59526d61b4728.shtml

2、关于实施个人信息保护认证的公告

11 月 18 日，国家市场监督管理总局、国家互联网信息办公室发布《关于实施个人信息保护认证的公告》，指出按照《个人信息保护认证实施规则》实施认证。

实施规则规定了个人信息保护认证的适用范围、认证依据、认证模式、认证实施程序、认证证书和认证标志、认证实施细则、认证责任等内容。其中，明确指出个人信息处理

者应当符合 GB/T 35273《信息安全技术 个人信息安全规范》的要求，对于开展跨境处理活动的个人信息处理者，还应当符合 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》的要求。

https://gkml.samr.gov.cn/nsjg/rzjgs/202211/t20221118_351801.html

3、北京、天津、浙江、江西互联网信息办公室发布关于报送2022年度汽车数据安全管理情况的通知

11 月 16 日起，天津市、北京市、北京市、浙江省网信办先后发布关于报送 2022 年度汽车数据安全管理情况的通知，对报送范围、报送内容、报送方式等内容进行明确，并提供《汽车数据安全管理情况报告（模板）》。

https://finance.sina.com.cn/jjxw/2022-11-17/doc-imqqsmrp6579871.shtml

4、深圳数据交易所正式揭牌

11 月 15 日，深圳数据交易所正式揭牌，并发布了深圳数据要素市场及数据交易系列成果。交易所以建设国家级数据交易所为目标，目前已汇聚市场参与主体 484 家，累计交易金额超 11 亿元。

https://www.sznews.com/news/content/2022-11/16/content_25458945.htm

5、深圳市地方标准《公共数据安全要求》发布

11 月 16 日，由深圳市信息安全管理中心与全知科技（杭州）有限责任公司牵头编制的深圳地方标准 DB4403/T 271-2022《公共数据安全要求》已于 11 月 14 日发布，并将于 12 月 1 日实施。《公共数据安全要求》在数据安全管理机构与人员机构管理中提到机构管理应设立数据安全管理机构，明确数据安全责任人，落实数据安全保护责任；应按照相关法律、法规、规章的要求编制公共数据资源目录，加强数据安全保护。

https://sz.oeeee.com/html/202211/21/1307002.html

6、印度新版《数字个人数据保护法（2022）》发布

近日，印度电子和信息技术部正式发布了新版《数字个人数据保护法（2022）》（Digital Personal Data Protection Bill 2022），该法案取消了之前的旧版《个人数据保护法案（2019）》中的数据本地化要求，将允许数据的跨境转移和在批准的可信任国家和地区存储。该法案还取消了对数据泄露事件的刑事处罚，取而代之的是：对未能采取 "合理的安全保障措施

"来防止个人数据泄露的实体将被罚款高达 250 亿卢比，需要重点考量每次数据泄露受影响用户的总人数。

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

技术、产品与市场

1、IDC：2021 年中国数字政府 IT 安全硬件市场规模达 64.9 亿

市场研究机构 IDC 发布的《中国数字政府 IT 安全硬件市场份额，2021》报告显示，2021 年中国数字政府 IT 安全硬件市场的规模达到 64.9 亿元人民币，同比增长 31.5%，整体市场呈现快速增长的态势，2021 年中国数字政府 IT 安全硬件市场竞争主要以综合性安全厂商和专业技术领域安全厂商为主。

IDC《中国数字政府 IT 安全软件市场份额，2021》报告显示，2021 年中国数字政府 IT 安全软件市场的年增长率为 37.7%，市场规模为 54.85 亿元人民币，**增长主要受益于云安全、数据安全及终端安全市场的大量需求**，相比 2020 年有较大增长。

https://www.anquanke.com/post/id/283309

2、华控清交：使用业界首款半同态加密芯片加速联邦学习

联邦学习致力于解决多方建模或预测等问题。主流的联邦学习方法是基于密文梯度的交换与融合，且此过程借助了半同态加密的性质。而半同态算法的加密、解密和同态运算

都极其耗费算力，在很多场景下甚至成为联邦学习的性能瓶颈。

华控清交研发了业界首款半同态计算加速卡 TsingJ Homomorphic Processing Card X1（以下简称“TsingJ X1”），能够高效解决半同态计算的性能问题，大幅提升半同态计算效率。具体而言，无论是联合建模还是联合预测，两块 TsingJ X1 加速卡相对单颗 AMD 旗舰 CPU 而言能让每个参与方的计算性能提升 5 倍左右。

https://mp.weixin.qq.com/s/XOmBbIIqk5YhajU78jlzBQ

3、研究：全球医疗机构因勒索软件攻击累计停机超 7 千天，造成经济损失 920 亿美元

据研究调查，**自 2018 年以来，全球已发生 500 次公开确认的针对医疗保健组织的勒索软件攻击。凶猛的攻势导致近 13000 个独立设施瘫痪，并影响到近 4900 万份病患记录**。

总体估算，我们认为这些攻击仅由停机造成的经济损失就已超过 920 亿美元。

尽管 2022 年针对医疗保健组织的勒索攻击数量有所下降，但这并不代表威胁程度有所降低。可以看到恶意黑客**提出的赎金数字和造成的停机时间愈发可观**，而且黑客可能也在**选取更具针对性的攻击方法**，确保用更广泛的破坏力提升

收到赎金的机率。此外，**针对系统进行加密锁定和数据窃取的“双重勒索”也愈发多见**。

勒索软件攻击有所减少的另一个原因（此趋势在美国乃至全球各行业均有体现）在于，**组织对于遭受攻击的态度越来越“低调”**。

https://www.secrss.com/articles/49153

4、Twitter 源代码表明，端到端加密私信即将到来

据 BleepingComputer 11 月 16 日消息，Twitter 正准备为其平台上用户之间的私信 (DM) 添加端到端加密 (E2EE)，预计这一功能将很快到来。

这是一项广受欢迎且需求量很大的功能，它将有助于进一步保护通信双方的私密性，免受任何第三方甚至是法律请求的影响。

早在 2018 年，Twitter 就曾尝试推出 E2EE 系统的原型，并将其命名为“秘密对话”（Secret Conversation），但随后就没有了下文。而最近，移动研究员 Jane Manchun Wong 发推称，她发现 Twitter 的安卓版源代码中出现了关于 E2EE 的内容。在一个字符串中，出现了“这个号码是根据你这次对话的加密密钥生成，如果它与接收者手机中的号码相匹配，就能保证端到端加密”的描述。

在 Twitter 的案例中，Wong 提到了“对话密钥”（conversation key），因此实施的 E2EE 方法可能是“对称的”，这意味着聊天中的两个人都使用相同的密钥进行加密和解密。发件人的消息在传输过程中被转换成不可读的密文，因此任何中间人，如互联网服务提供商、黑客，甚至 Twitter 本身，都无法读取消息内容。

https://www.bleepingcomputer.com/news/security/twitter-source-code-indicates-end-to-end-encrypted-dms-are-coming/

5、谷歌将于 2023 年在安卓 13 中引入隐私沙盒

谷歌宣布将从明年初开始向运行 Android 13 的移动设备推出 Beta 版 Android 隐私沙盒。隐私沙盒旨在创建技术来保护人们的在线隐私，限制秘密跟踪。

隐私沙盒的目标是：

- 建立新技术来保障用户信息的私密性；
- 使发布者和开发者能够在不依赖侵入性跟踪的情况下保持在线内容免费；
- 与业界合作建立新的互联网隐私标准。

安卓隐私沙盒取代了跨 APP ID，并用属性报告（Attribution Reporting）、主题（Topics）、FLEDGE 等 API 系统来实现相关信息的记录。这些 API 合起来取得了目前安卓

系统中使用的广告 ID（advertising ID），缓解了 advertising ID 被用于追踪用户的问题。

SDK Runtime 可以隔离第三方广告代码，因此 APP 将不再包含在其代码中。也无法访问用户兴趣和其他营销相关的数据。

总体来说，隐私沙盒在一定程度上实现了隐私保护的改进。

https://www.freebuf.com/articles/350028.html

业界观点

1、肖远企：不断强化金融科技监管建设，确保金融科技安全稳健发展

10 月 31 日，中国银保监会副主席肖远企在“2022 年香港金融科技周”活动上发表演讲。他表示，金融科技是当前全球金融业共同面对的一项重要命题，并将不断发展、变化和演进。

对此，肖远企表示银保监会在不断强化金融科技监管建设，完善监管规则和机制，丰富监管方式和手段，确保金融科技安全稳健发展：

一是完善基于规则的监管。我们坚持金融业务必须持牌经营的原则，将所有金融活动纳入金融监管，持续完善修订现行金融监管规定，针对新兴的金融科技活动及时制定出台专门审慎监管规则。

二是丰富金融科技监管工具。在监管科技方面，持续推进现场检查和非现场监测的数字化体系建设。在合规科技方面，我们鼓励金融机构积极探索建设数字化平台，强化对合规风险的有效管控。目前，大型银行均已建立合规科技信息系统，中小银行也正在加快建设步伐。

三是加强消费者保护。我们非常关注金融科技及其创新

对公众利益的影响。我们始终认为，在金融科技发展的进程中，加强金融消费者权益和数据安全保护、强化信息披露同样至关重要。

https://mp.weixin.qq.com/s/PFPUBFdbk4WxxFWGaAlp6A

2、刘进：数据安全需切换视角 从网络攻防到保护重要数据资产

11 月 15 日，在 2022 中国互联网大会开幕论坛上，奇安信集团副总裁刘进在主题演讲时指出，大数据环境下，业务与数据流转更为复杂，需要数据安全管理与技术相结合，从组织、制度、流程上完善数据安全管理体系，有效支撑数据安全技术与运营更好落地。

他指出，根据政企机构数字化程度和安全建设的不同阶段，数据安全的重点也有不同，需要分三个阶段、六个步骤有序实施建设：

第一阶段是盘家底、补短板。围绕重要数据资产进行基础安全防护，提高整体防护水平，外防攻击，内防违规，掌控全局。

第二阶段是分类分级，体系规划。安全建设相对完善、数字化程度高的政企机构可以从这一阶段开始，对数据进行系统治理、分类分级，然后进行体系化规划，制定战略目标、

设计体系架构、管理体系、技术体系和运营体系。

第三阶段是有序建设和促使运营阶段。在做好前两个阶段的基础上，这一步重点是以保护数据资产为核心，将防护措施落地实施，做好联防联控、持续运营。通过实战化运营，真正做到“业务不中断、数据不出事、合规不踩线”。

https://software.it168.com/a2022/1115/6775/000006775217.shtml

3、刘东：认证制度为中国个人信息跨境流动保驾护航

2022 年 11 月 18 日，为贯彻落实《中华人民共和国个人信息保护法》有关规定，根据《中华人民共和国认证认可条例》，国家市场监督管理总局、国家互联网信息办公室决定实施个人信息保护认证，鼓励个人信息处理者通过认证方式提升个人信息保护能力。官方公告:《关于实施个人信息保护认证的公告》。

随着互联网在全球的普及和数字经济在全球的发展，数据跨境流动已经成为各个国家和地区重点关注的议题。个人信息的跨境流动同时具备个人权益保护、企业合规发展和各国监管合作与博弈三个维度，各国和地区近年来对个人信息的跨境流动高度重视，相继出台和完善法律规则和监管框架。对此，我国《个人信息保护法》建立了既能化解风险、又可

面向全球的个人信息跨境流动制度体系。国家市场监督管理总局、国家互联网信息办公室制定的《个人信息保护认证实施规则》中关于个人信息跨境提供认证制度的规定，明确了《个人信息保护法》第三十八条第二款规定的“按照国家网信部门的规定经专业机构进行的个人信息保护认证”的适用情形、基本原则、基本要求等规定，对保护个人信息主体权益、促进数字经济发展具有重要意义，是我国个人信息跨境流动制度体系进一步完善的重要标志。

https://www.secrss.com/articles/49143

4、保障数据安全有序跨境流动

数字服务贸易，一般指数字技术与服务贸易融合产生的新业态新模式。近年来，我国数字服务贸易发展迅速，要持续推进数字服务贸易的高质量发展，离不开一个前提，即其依赖的关键性要素“数据”必须是安全可靠的。因此，可从监管、技术创新、国际标准制定等多个角度入手，在发展数字服务贸易的过程中，合理科学地保障数据有序、安全、积极地实现跨境流动。

其一，完善数据流动顶层设计，明确数据安全监管责任。对于跨境经营数字服务的企业，需出台有关法律，规定相关权利与责任，要依据不同类型数据的敏感程度与风险程度，

明确数据跨境流动规则。还应通过不断完善数据安全评估流程与数字服务行业规范，提升国家对数据资源的监管水平。

其二，加快数字技术创新进程，提升数据风险应对能力。要谨慎应对技术带来的数据安全风险，比如，在区块链技术的应用中，警惕公钥与私钥信息的传播与使用，明确数据管理权限，避免数据泄露。为了确保数据资源在数字服务贸易过程中的完整性、保密性和可用性，数字技术的创新与应用尚需学界与业界的共同努力。

其三，提升国际竞争力，参与相关标准制定。数字服务贸易与数字技术成熟发展、经济全球化场景息息相关，我国应当积极参与相关国际标准制定，在倡导合作共识的基础上争取主动权。

http://www.ce.cn/cysc/newmain/yc/jsxw/202211/17/t20221117_38234423.shtml

5、李国杰：算力是数字时代的重要生产力

据中国信息通信研究院发表的《中国算力发展指数白皮书》显示,通过国家投入产出表模型计算,2020 年以计算机为代表的算力产业规模达 2 万亿元,直接带动经济总产出 1.7 万亿元,间接带动经济总产出 6.3 万亿元,即在算力中每投入 1 元,平均将带动 3—4 元经济产出。

据统计,截至今年 6 月底,我国数据中心机架总规模超过 590 万标准机架,服务器规模约 2000 万台,算力总规模超过 150EFlops(每秒 1.5 万京次浮点运算次数),位居全球第二。

今年 2 月,国家发展改革委等部门联合印发通知,同意在京津冀、长三角、粤港澳大湾区、成渝、内蒙古、贵州、甘肃、宁夏等 8 地启动建设国家算力枢纽节点,并规划了 10 个国家数据中心集群。我国一体化大数据中心体系完成总体布局设计,“东数西算”工程正式全面启动。东数西算”是继“西气东输”“西电东送”“南水北调”后又一项国家重要战略工程。作为一项国家级算力资源跨域调配战略工程,“东数西算”工程对于优化我国算力资源空间布局,加快打造全国算力“一张网”,构筑我国数字经济发展新优势具有重要意义。深入推进“东数西算”工程,并不是简单的算力堆砌,而是要实现网络、算力调度、产业链、数据要素治理等各方面资源协同,强化东西部跨域统筹发展。

http://www.ciia.org.cn/news/19304.cshtml

数据安全事件

1、谷歌将支付 3.91 亿美元解决关于 Android 位置跟踪的诉讼

据媒体 11 月 14 日报道，谷歌已同意支付 3.915 亿美元，来解决美国 40 个州提起的关于隐私的诉讼。俄勒冈州总检察长称，谷歌误导用户以为自己在账户设置中关闭了位置跟踪，而事实上它仍在收集他们的位置信息。此次和解还要求谷歌引入更多用户友好型的账户控制，并限制公司对某些类型位置数据的使用和存储。澳大利亚 ACCC 曾在 8 月对谷歌处以 6000 万美元的罚款，原因是它使用相同的方法收集澳大利亚用户的位置数据近两年。

https://www.bleepingcomputer.com/news/google/google-will-pay-391m-to-settle-android-location-tracking-lawsuit/

2、勒索软件团伙公布法国军工巨头泰雷兹内部敏感数据

11 月 16 日消息，法国航空航天、国防与安全巨头泰雷兹集团发布声明称，勒索软件团伙 LockBit 3.0 公布了与该公司有关的数 GB 数据，但集团自身并未发现 IT 系统遭受入侵的证据。

网络犯罪组织 LockBit 上周发布了一个 9.5 Gb 大小的归

档文件，其中明确包含来自泰雷兹集团的信息。恶意黑客此前曾宣布，除非泰雷兹方面支付赎金，否则他们将公开文件内容。

泄露的文件似乎包含技术和集团业务文件。黑客方面称已掌握涉及公司运营的高度敏感信息，以及“商业文件、会计文件、客户文件、客户结构图和软件。” 泰雷兹集团称确实发生了安全违规事件，但受影响的并非自身系统。内部安全专家提出了泄露的两个可能来源，其一被确认为合作伙伴在专用协作门户上的账户，这可能导致“部分受限信息”的泄露。

https://www.secrss.com/articles/49050

3、俄罗斯数据泄露频发：共享踏板车平台 720 万用户数据被出售

11 月 16 日报道，近日，黑客开始在黑客论坛上出售包含 720 万客户详细信息的数据库后，俄罗斯踏板车共享服务 Whoosh 确认发生数据泄露。据悉，Whoosh 是俄罗斯领先的城市出行服务平台，在 40 个城市运营，拥有超过 75,000 辆电动滑板车。

一名威胁行为者开始在黑客论坛上出售被盗数据，据称其中包含可用于免费访问该服务的促销代码，以及部分用户

身份和支付卡数据。该公司本月早些时候通过俄罗斯媒体的声明证实了网络攻击，但声称其 IT 专家已成功阻止了攻击。

在今天与 RIA Novosti 分享的一份新声明中，Whoosh 承认存在数据泄露，并告知其用户群他们正在与执法当局合作，采取一切措施阻止数据的分发。Whoosh 的一位发言人表示："此次泄露并未影响敏感的用户数据，例如账户访问、交易信息或旅行详情。我们的安全程序还排除了第三方获取用户银行卡全部支付数据的可能性。"

https://www.secrss.com/articles/49007

4、马来西亚选举委员会的数据库泄露近 80 万选民的信息

11 月 11 日报道称，马来西亚约 80 万名选民的个人信息泄露。据称，泄露的 67 GB 数据泄露来自选举委员会的数据库，该数据库目前在一个暗网市场上以 2000 美元的价格出售。11 月 10 日，研究人员在 lowyat.net 发现了出售的信息，涉及居民的姓名、身份证号码、邮件地址、出生日期和家庭住址等。据称，这些数据是从选举委员会的 MySPR 网站上窃取的。这一泄露事件发生在 11 月 19 日全国投票前一周，引起了马来西亚居民的担忧。

https://www.nst.com.my/news/crime-courts/2022/11/849700/personal-info-800000-voters-compromised-alleged-breach-ec-database

5、医疗索赔处理公司服务器暴露了 60 万名囚犯的 PHI

11 月 16 日，据外媒报道，总部位于肯塔基州的 CorrectCare Integrated Health Inc.因服务器配置错误而导致的“未经授权的访问/披露”违规行为，暴露了近 60 万名囚犯的敏感信息，这些囚犯在过去十年中在监禁期间接受了医疗护理。

该公司表示，它在 7 月 6 日发现 CorrectCare 网络服务器上的两个文件目录已“无意中”暴露在互联网上，文件目录包含被关押在州立监狱的个人的受保护健康信息（PHI），暴露的文件目录中包含的患者信息包括全名、出生日期、社会安全号码和有限的健康信息，例如诊断代码和程序代码。https://www.inforisktoday.com/misconfigured-server-exposed-phi-600000-inmates-a-20482

6、数百个亚马逊 RDS 泄露了用户信息

11 月 17 日报道，安全公司 Mitiga 最新发现显示，亚马逊关系型数据库服务（Amazon RDS）上数百个数据库正在暴露用户个人身份信息（PII）。

安全研究员 Ariel Szarf、Doron Karmi 和 Lionel Saposnik 在与 The Hacker News 分享的报告中表示，泄露的

数据库中包含用户姓名、电子邮件地址、电话号码、出生日期、婚姻状况、汽车租赁信息，甚至是公司登录信息，如此详细的用户数据，为潜在攻击者提供了丰富的“素材”。

亚马逊 RDS 是一项 Web 服务，可以在亚马逊网络服务（AWS）云中建立关系型数据库。此次亚马逊 RDS 用户个人数据泄漏事件源于一个称为公共 RDS 快照的功能，该功能允许创建一个在云中运行数据库的环境备份，并且可以被所有 AWS 账户访问。

https://www.freebuf.com/articles/350099.html

7、卡塔尔世界杯应用程序带来数据安全和隐私噩梦

11 月 6 日报道，鉴于数以万计配备人脸识别技术的监控摄像头被强制要求下载间谍软件，将在卡塔尔举行的世界杯看起来更像是一场数据安全和隐私噩梦，而不是一场华丽的体育比赛盛典。

据报道，足球迷及其他前往卡塔尔的人必须下载两个应用程序：Ehteraz 和 Hayya，前者是新冠疫情追踪程序，后者允许持票者进入体育馆，并享用免费的地铁和巴士交通服务。

Ehteraz 新冠疫情追踪程序甚至在世界杯使用之前就受到了密切关注，因为它允许当局远程访问用户手机中的图片和视频，可以在没有提示的情况下拨打电话。此外，Ehteraz

要求后台位置服务始终处于打开状态，从而使该应用程序能够对文件系统执行读写操作。

据称，Ehteraz 能够安装一个加密的文件，该文件声称含有使用该应用程序的其他设备的独特 ID、二维码、用户感染状态、配置参数和邻近数据。实际上，该应用程序显然私底下从最终用户那里获取数据。

https://mp.weixin.qq.com/s/srA9dVRTr6Z3-EgUwfIbLg

8、本溪银行因过失泄露信息，被罚 40 万

11 月 14 日消息，据央行近日公布的行政处罚信息公示表显示，本溪银行股份有限公司因过失泄露信息，被处以罚款 40 万元;时任该行普惠金融部直营中心代理经理郭佩强，因对上述行为负有直接责任，被处以罚款 7.1 万元。

在此之前，本溪银行就因出现“内鬼”与他人内外勾结，一年售卖 915 份征信报告，通过售卖客户个人信息非法获利 23.23 万元而受到监管处罚。

https://mp.weixin.qq.com/s/hSCAhUWCmxRKccV7q1jnZQ

9、Instagram 凭据网络钓鱼攻击绕过 Microsoft 电子邮件安全，泄露用户凭据

11 月 18 日，据外媒报道，针对国家教育机构的学生而

发起的一场冒充 Instagram 凭证网络钓鱼攻击，影响了 22,000 人。

该电子邮件似乎来自 Instagram 支持，发件人姓名、Instagram 和电子邮件地址与 Instagram 的真实凭据相匹配。

一旦用户点击电子邮件中的链接，就会打开一个虚假的登录页面，其中包括 Instagram 品牌和检测到的异常登录尝试的详细信息，以及一个“这不是我”按钮。单击该按钮后，受害者将被引导至第二个虚假登录页面，该页面旨在泄露敏感的用户凭据。

“电子邮件攻击使用语言作为主要攻击媒介，并绕过原生的 Microsoft 电子邮件安全控制。它通过了 SPF 和 DMARC 电子邮件身份验证检查，”安全研究人员解释说。

https://www.infosecurity-magazine.com/news/instagram-credential-phishing/?&web_view=true

10、英国：萨福克郡警方不小心在网站上发布了受害者的数据

11 月 16 日，据外媒报道，在受害者的个人详细信息出现在警方网站上后，针对萨福克警方的调查已经开始。

《East Anglian Daily Times》媒体称，公布的信息包括受害者的姓名、地址、出生日期和所犯罪行的详细信息，据报

道它影响了“数百人”。

“警方已获悉，一些不应该上传的个人信息通过警察网站被公开访问。此事很快得到解决，信息无法再访问。我们非常重视《数据保护法（Data Protection Act）》规定的义务。”萨福克警方表示道。

https://www.bbc.com/news/uk-england-suffolk-63634650?&web_view=true

《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： 钟力、唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nelab@360.cn

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