全球数据安全观察

总第 115 期 2022 年第 43 期

(2022.11.21-2022.11.27)

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、证监会发布《证券期货业机构内部接口 证券交易》等 7 项金融行业标准

近日，证监会发布《证券期货业机构内部接口 证券交易》《证券业登记结算核心术语》《证券期货业数据安全管理与保护指引》《证券期货业信息技术服务连续性管理指南》《场外通用传输接口》《证券公司客户信息交换规范》《证券经营机构投资者适当性管理 投资者评估数据要求》7 项金融行业标准，自公布之日起施行。

其中,《证券期货业机构内部接口 证券交易》有利于规范证券交易数据接口，促进跨机构、跨系统的证券交易数据共享。

《证券期货业数据安全管理与保护指引》从数据安全管理基本原则、组织架构、制度、技术等方面提供指引，规范行业机构开展数据安全管理和保护工作，提升行业数据安全管理水平，适用于证券期货业机构开展数据安全管理与保护工作的参考和指引。

《场外通用传输接口》有利于市场参与机构快捷、方便地实现各类业务系统端到端的数据传输，降低数据通信成本，提高行业数据通信安全水平和通信效率。

《证券公司客户信息交换规范》有利于提高客户信息交互规范性与时效性。

http://www.csrc.gov.cn/csrc/c100028/c6550574/content.shtml

2、《北京市数字经济促进条例》表决通过

11 月 25 日，北京市第十五届人民代表大会常务委员会第四十五次会议表决通过《北京市数字经济促进条例》，自 2023 年 1 月 1 日起施行。

条例规定了数字产业化的技术、产业方向和企业发展目标，产业数字化列举了数字化转型提升的产业领域及推动措施。在数字治理方面，条例还规定了完善平台企业自我治理和政府治理，健全数据安全管理和个人隐私保护。

https://www.163.com/dy/article/HN23RA140512D3VJ.html

3、《广西壮族自治区大数据发展条例》通过

11 月 25 日，《广西壮族自治区大数据发展条例》已经自治区第十三届人大常委会第三十四次会议通过，并于 2023 年 1 月 1 日起施行。这是广西第一部数据领域地方性法规。

关于数据安全保障，条例提出具体要求，包括实行数据安全责任制、明确对数据进行分级分类管理以及对公共数据进行安全监测、应急处置、安全备份、安全协作、安全销毁

等体系建设等。

https://www.vfuw.cn/news-41523-1.html

4、《杭州市深化数字政府建设实施方案》印发

近日，《杭州市深化数字政府建设实施方案》印发，在构建数字政府全方位安全保障体系部分，提出要进一步强化政府部门数据安全管理职责，健全网络安全工作责任体系；强化网络安全、数据安全监管；加强对参与政府信息化建设与运营企业的规范管理；构建数据安全防护能力评估指标体系；严格落实公共数据安全制度规范体系；完善公共数据安全技术防护体系等。

https://www.hangzhou.gov.cn/art/2022/11/8/art_1229063387_1827091.html

5、《工业互联网密码支撑标准体系建设指南》《车联网（智能网联汽车）密码支撑标准体系建设指南》正式发布

近日，《工业互联网密码支撑标准体系建设指南》《车联网（智能网联汽车）密码支撑标准体系建设指南》正式发布。

《工业互联网密码支撑标准体系建设指南》明确了工业互联网密码支撑标准体系建设思路及目标，提出密码应用共性、设备密码应用、控制系统密码应用、网络密码应用、边

缘计算密码应用、平台密码应用、数据密码应用、密码行业应用、密码应用管理与支撑等九个方面的标准建设内容，对加快指导研制工业互联网密码应用标准，强化工业互联网安全防护能力，推动工业互联网产业高质量发展具有重要支撑作用。

《车联网（智能网联汽车）密码支撑标准体系建设指南》从基础共性、智能网联汽车、信息通信、服务与平台、智能交通、密码应用管理与支撑等六个方面构建车联网密码应用标准体系，进一步明确了建设思路及目标，用于指导相关标准研制，为规范车联网（智能网联汽车）密码应用，保障车联网（智能网联汽车）安全，促进车联网（智能网联汽车）产业高质量发展保驾护航。

https://www.secrss.com/articles/49364

技术、产品与市场

1、研究：核部门受到暗网上数据泄露的威胁

暗网充满了数据泄露，其中包含来自关键基础设施公司（包括核设施）的敏感数据。一位网络分析师声称这是俄乌战争的连锁反应。

暗网监控公司 Cyble 表示，威胁行为者和黑客组织利用乌克兰战争扩大了他们的攻击服务范围。通常，它们以关键基础设施为目标并泄露敏感文件，包括个人身份信息 (PII)。

Cyble 的研究表示，针对全球核工业的网络犯罪活动有所增加。从今年 2 月开始，在网络犯罪论坛和暗网上至少发现了 8 起泄密事件，目标是俄罗斯、巴西、伊朗、台湾、印度尼西亚、泰国、印度和南非的核设施。“即使核设施旨在进行气隙隔离，但配置错误的网络、暴露的资产以及具有网络和社会工程攻击的易受攻击的 IT/OT 设备在发起网络攻击时仍可被视为关键因素。”

https://cybernews.com/cyber-war/nuclear-data-leaks/

2、谷歌启用抗量子密码

11 月 19 日，谷歌宣布，Google Cloud 已经在内部 ALTS 协议上启用了抗量子密码(或 PQC)，避免未来黑客使用量子

运算技术，破解当前经加密的资料。Google 提到，目前美国国家标准与技术研究院（NIST）仍未决定后量子密码（Post-Quantum Cryptography，PQC）标准，也因为目前的后量子算法仍属于临时性质，所以 Google 内部的 ALTS 便成为了良好的试验对象，借由控制所有端点抵御先存储后解密攻击，同时，当未来 NIST 决定采用不同的标准，Google 也可以相对简单地进行切换。

https://www.secrss.com/articles/49263

3、工信安全中心发布《中国数据要素市场发展报告（2021-2022)》

报告围绕数据要素市场培育过程中，政府主管部门及数据要素流通涉及主体各方面临的难点及问题，梳理了数据要素相关类别及其采集、存储、加工、流通、分析等环节的相关特性，从宏观经济增长、行业发展、企业绩效三个层面估算了数据要素的经济贡献度；基于数据要素市场化过程各相关主体交易及流通模式总结，建立了中国数据要素市场化指数模型，定量分析了各地区数据要素市场化发展程度；围绕数据要素流通体系的流通交易模式、服务创新模式、生态汇聚模式进行了总结梳理，并介绍了相关典型案例；最后，针对我国当前发展现状，提出未来数据要素市场的发展趋势和

展望。

报告提出，2021 年我国数据要素市场规模达 815 亿元，预计“十四五”期间市场规模复合增速将超过 25%，整体将进入群体性突破的快速发展阶段。从宏观经济增长层面来看，数据要素对 2021 年 GDP 增长的贡献率和贡献度分别为 14.7%和 0.83 个百分点；从行业发展层面来看，数据要素对各个行业的产值影响具有较大差异，其中，信息传输、软件和信息技术服务业产出对数据要素最为敏感；从企业绩效层面来看，数据要素显著提升企业总资产净利润率，数字化转型对于制造业企业的影响最大。

https://www.secrss.com/articles/49382

4、《中国政企机构数据安全风险分析报告》发布

《报告》显示，2022 年 1 月-2022 年 10 月，安全内参共收录全球政企机构重大数据安全报道 180 起，其中数据泄露相关安全事件高达 93 起，占 51.7%。与近三年平均每月公开报道频次相比，2022 年相较前三年全球重大数据安全相关事件数量有小幅下降，略低于 2020 年与 2021 年。

并且，**数据泄露已经超越数据破坏成为数据安全最大风险**。与 2021 年相比，从数量来看，2021 年全球数据安全大事件，涉及数据破坏的有 102 件，占总量的 42.0%；涉及数

据泄露的有 100 件，占总量的 41.2%。2022 年，全球数据安全大事件涉及数据破坏的大事件下降至 42 件，占总量的 23.3%；而数据泄露事件有 93 件，占 51.7%。可见近两年来，由于数据破坏导致的数据安全事件数量大幅减少，同时，数据泄露类事件一直较为严重。

从政企机构重大数据安全事件发生的原因来看，2022 年 1 月~2022 年 10 月，**超过五成安全事件是由于外部攻击（指没有获得认证的、未经授权的非法用户对内网进行的访问请求或攻击行为）导致的**，但也有 5.0%的事件是由于内部人员违规操作。3.9%的重大数据安全事件是由于存在漏洞。

https://mp.weixin.qq.com/s/eTeLnp4g8J4yKAIUAWYJIw

5、SSH 公司推出全球首款用于大型机的量子安全数据通信软件

11 月 24 日消息，SSH 公司宣布即将推出全球首款用于大型机的量子安全数据通信软件 Tectia SSH Server for IBM z/OS。通过量子安全升级，该软件可以与 6 月发布的 Tectia 客户端/服务器及相关第三方应用程序进行通信，创建安全远程访问、文件传输以及大型机出入连接隧道，从而实现大型机用户的文件传输、终端连接具有量子安全性能。

https://mp.weixin.qq.com/s/JRSTXQB6tADcjFJnq8jGBg

业界观点

1、马树娟：用认证为个人信息加道“安全锁”

为规范个人信息处理活动，促进个人信息合理利用，近日，国家市场监管总局、国家网信办发布《个人信息保护认证实施规则》(以下简称《规则》)，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。

所谓认证，是指由具备专业能力的第三方机构，依据相关标准或技术规范，对企业的产品、服务和管理体系等进行评定。为了规范个人信息处理活动，2021 年我国出台了个人信息保护法，其中明确规定，推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务。此次《规则》的发布，既是对个人信息保护法的贯彻落实，也是引入第三方专业力量加强个人信息保护的有益尝试。对企业来说，主动就自身个人信息保护工作进行认证，不仅可以增强自身相关工作的合规性，而且可以让相关各方直观了解自身个人信息保护水平，增加对自己的信任，从而在市场竞争中赢得更多机会。当然，获得认证证书并不意味着一劳永逸，《规则》特别明确，认证机构应采取合理频次、适当方式实施监督，确保获得认证者持续符合认证要求，这就相当于给企业个人信息保护工作加了道“安全锁”。对老百姓来说，

通过查看企业有无个人信息保护认证证书，也能给自己的消费决策提供重要参考。

https://mp.weixin.qq.com/s/lLSU0O2sPkI93bJ85gvD3Q

2、陈志刚：数据安全与使用是硬币的两个面，实现平衡要靠制度和技术

日前，《国务院关于数字经济发展情况的报告》（以下简称报告）提请十三届全国人大常委会第三十七次会议审议。《报告》显示，我国数字经济总体规模连续多年位居世界第二，对经济社会发展的引领支撑作用日益凸显，信息通信专家陈志刚对此进行了解读。

陈志刚把数据安全与数据使用比喻成一个硬币的两个面，“需要在合法合规的前提下做到平衡，不能以安全的名义阻碍数据要素的流通，更不能以流通的名义放弃安全，实现平衡要靠制度和技术两个引擎：

一是在制度层面，要遵循数据相关法律法规和标准，并不断创新制度规则，以促进流通使用为原则、不流通不使用为例外进行建构；

二是在技术层面，要不断创新数据流通利用技术和业务模式，例如探索数据共享新技术——全同态加密、差分隐私、函数加密零知识证明、安全多方计算的应用，用技术赋能制

度建设。”

https://www.163.com/dy/article/HMPTBSMK0514D3UH.html

3、赵鞶：坚持健康医疗数据安全与发展并重

为推动全民健康信息化建设，近日发布的《“十四五”全民健康信息化规划》对关键信息基础设施安全、数据安全防护能力、密码安全免疫体系提出系列要求。

健康医疗数据是我国重要的基础性战略资源，坚持健康医疗数据安全与发展并重，是全民健康信息化高质量发展的必经之路。要根据《规划》要求，制定数据分类分级指南，确定核心数据、重要数据和一般数据目录，落实数据安全法规制度和标准，严格核心数据管控，加强重要数据保护，规范一般数据管理。

在重要数据和个人信息保护方面，要重点保护大规模个人信息和敏感个人信息;加强数据出境安全评估、监测和检查，及时发现安全隐患。在安全监测与应急处置方面，要建设数据安全态势感知平台，强化技术检查监测手段建设，组建行业专门技术支撑机构，落实风险评估、监测预警和应急处置等制度，提升网络安全和数据安全保护能力。

在数据安全人才培养方面，要通过开展行业网络安全比

武竞赛、攻防演练等，提升行业实战对抗能力，加强行业数据安全人才培养。加强信息化知识普及和法规宣贯，组织教育培训，提高全行业人员信息素养以及网络安全、个人信息保护的能力。与此同时，要推动关键技术研发和应用，运用人工智能、区块链等新一代信息技术进行数据安全防护。

密码安全是筑牢网络安全的基石。《规划》要求构建行业网络可信体系，全面推广商用密码应用，完善卫生健康行业商用密码应用体系;要建设可信数字身份管理系统，实现医患可信身份电子认证和电子签名，确保网络行为可管、可控、可溯源，同时实现电子认证服务跨域互信互认。

https://www.chima.org.cn/Html/News/Articles/15913.html

4、Gartner：开展数据安全治理的四个步骤

Gartner 预测，到 2025 年，国内 60%以上企业机构的董事会，将把网络安全风险视为一种业务风险。这个趋势，会帮助企业把网络安全投资以及数据安全投资从合规型驱动转换成业务型驱动。

Gartner 提出数据安全治理理念，帮助企业从合规驱动型的数据安全投资，转向业务驱动型的安全投资。该理念需要四个步骤:

第一步，设置数据安全与管理职能。涉及企业的角色分

工以及企业内部数据安全管理体系建设，日常运营的流程以及操作等标准模板。

第二步，落实数据发现与分级分类。包括数据的类型以及存储的位置，根据数据使用的敏感性和数据的业务属性进行分类分级。

第三步，开展数据安全与合规评估。《数据安全法》要求："涉及重要数据处理，定期要开展一次数据安全风险评估。涉及数据出境，需要做数据出境安全评估。涉及处理个人信息，也要做个人影响评估。"因此，企业需要长期持续运营投入成本，来进行评估工作。

第四步，选择并整合数据安全产品。Gartner 推荐企业在选择数据安全产品时，尽量采用整合型的数据安全产品，而不用花费大量精力来长期操作、维护单一功能的数据安全产品。

https://www.51cto.com/article/740398.html

5、观点：没有人可以拥有数据？

德国公法教授协会的成员 Lothar Determann 分析并权衡了数据产权化对保护创造力和技术进步以及个人隐私等方面的影响，主要包括：

（1）数据产权无助于创造性和技术进步。数据产权的建

立是否会鼓励公司分享和交易数据却还远未确定。同时，数据产权化可能会对激励创造力或技术进步产生负面影响，将新的产权授予数据最终只会像专利和版权一样，成为大企业敛财的工具。

（2）数据产权无助于保护个人隐私。再赋予数据主体从财产法规定的数据收集或使用排除权（产权），充其量只是一种重复，且这种权利在保护人类尊严和个人隐私方面远不如现行的数据隐私法。

（3）赋予数据产权破坏了表达自由。允许个人或公司控制对其数据访问的数据产权化会限制数据收集，从而阻碍信息的自由流动。

（4）限制信息流动也会严重阻碍公共管理和执法。个人可能会将政府排除在数据之外，进而阻碍了公共政策的透明度和问责制。

（5）数据产权化限制了竞争。当数据所有者是数据的“唯一来源”时，所有者将不受价格上限的限制，从而导致数据的垄断，损害竞争。

（6）数据产权化是对社会公平正义的破坏。如果公司因为他们无法运行以数据为基础的服务模式而不得不转向付费模式，那么大部分人可能会失去获得服务的机会。

（7）数据产权制度面临难以克服的实施障碍。数据产权

化后的实际生活中会产生很多繁琐的问题。

因此，Lothar Determann 认为数据的产权化并不利于促进更好的隐私或更多的创新或技术进步，而更有可能损害到言论自由、信息自由、科学和技术进步；同时，将数据产权化的政策在实施方面还存在许多难以逾越的障碍。所以，于当前将数据产权化的理由并不令人信服，而且远不及保持数据“开放”所带来之收益，所以我们并不需要为数据创造新的产权。

https://mp.weixin.qq.com/s/P_AO2NK3j6QFHJoB9Ctosw

数据安全事件

1、WhatsApp 数据大泄露，近 5 亿条用户号码在暗网出售

11 月 25 日，据 Cybernews 报道，有黑客正在地下论坛出售近 5 亿 WhatsApp 用户的最新手机号码，而通过检验数据库样本，这些数据极有可能是真实数据。

11 月 16 日，一名黑客在著名黑客社区论坛上发布了一则广告，声称出售 WhatsApp 2022 年数据库，库内包含 4.87 亿用户手机号码。

公开数据显示，WhatsApp 在全球拥有超过 20 亿月活跃用户。据称，该数据库包含 84 个国家的 WhatsApp 用户数据。威胁行动者称其中包含 3200 万美国用户、4500 万埃及用户、3500 万意大利用户、2900 万沙特阿拉伯用户、2000 万法国用户、2000 万土耳其用户信息；还包含近 1000 万俄罗斯公民和 1100 多万英国公民的电话号码。

WhatsApp 母公司 Meta 对此不予置评。Meta 长期以来因允许第三方收集用户数据而受到批评。通常情况下，发布在网上的大量数据转储是通过抓取获得的，此举违反了 WhatsApp 的服务条款。某黑客论坛上存在超过 5.33 亿 WhatsApp 用户纪录的泄露，下载数据库几乎免费。

https://www.freebuf.com/articles/database/350756.html

2、基于 Go 的恶意软件正在大肆窃取用户信息

11 月 24 日，据外媒报道，越来越多的网络犯罪集团转向名为 Aurora 的信息窃取恶意软件，该恶意软件基于 Go 开源编程语言，旨在从浏览器、加密货币钱包和本地系统中获取数据。

据研究人员称，到目前为止，已有 40 多个加密货币钱包和 Telegram 等应用程序成功成为目标，收集到的数据在各种市场上以高价提供给网络犯罪分子。

https://www.darkreading.com/threat-intelligence/hot-ticket-aurora-go-based-infostealer-favor-cyber-threat-actors

3、亚洲航空 500 万个人数据信息泄露，涉及姓名、身份证号码

11 月 23 日，据 The Hacker News 网站披露，马来西亚廉价航空公司-亚洲航空内部系统遭到勒索软件组织袭击，约 500 万名乘客和员工的个人数据信息泄露。

这次外泄的资料包括亚航乘客的身份证号码、姓名和订票编号。此外，亚航、泰国亚航和印尼亚航雇员的信息也被泄露。

黑客组织的发言人说，亚航有对攻击事件做出回应，但没有为防止资料外泄同他们商谈价钱，意味亚航无意付款给

黑客。

据悉，此次网络攻击背后黑手是名为 Daixin 的勒索软件团伙，该团伙在成功获取亚洲航空大量内部数据资料后，随即在其数据泄露网站上公开了部分数据样本。

https://www.secrss.com/articles/49293

4、某医疗机构公众号系统漏洞遭利用，攻击者窃取 10 余万条公民数据境外售卖被抓

11 月 21 日报道，近日，哈尔滨市公安局南岗分局网安大队民警在工作中发现，境外某黑客论坛上有一名用户于 2022 年 10 月发贴出售公民个人信息数据，自称持有数据量约 20GB，售价 0.2 比特币，该用户还公布了 29 条数据样本，样本中还包括了公民姓名、联系电话、家庭住址等个人信息。由于该线索涉及侵犯公民个人信息犯罪，且涉案数据量较大，立即引起了各级网安部门的高度重视。

10 月 22 日，南岗公安分局民警在哈尔滨市平房区将涉嫌非法获取计算机信息系统数据的犯罪嫌疑人麻某抓获，并在其电脑中查获非法获取的公民个人信息 10 万余条。经审讯，犯罪嫌疑人麻某供述，其为 IT 行业从业人员，利用某医疗机构微信公众号的系统漏洞，在今年 4 月至 10 月间，通过技术手段非法获取该计算机系统数据 10 万余条，而后在

境外某黑客论坛发帖出售，截至落网前，已非法获利 1500 美元。

https://www.secrss.com/articles/49228

6、湖南网信部门开出数据安全领域行政执法罚单

2022 年 11 月 19 日，在湖南省网信办的指导下，湘西州网信办依法对湘西州某县自来水公司作出行政处罚。这是《湖南省网络安全和信息化条例》自今年 1 月 1 日起正式施行以来，湖南网信部门开出的首张罚单。

该县自来水公司缴费系统因未采取相应防护措施履行数据安全保护义务，违反《湖南省网络安全和信息化条例》。湘西州网信办依据规定，对该县自来水公司予以警告和责令整改，并对公司法人作出罚款的行政处罚。该自来水公司负责人表示，真诚接受行政处罚，并按要求全面整改。

据介绍，此次在数据安全领域开展的行政执法活动，标志着湖南全省网信部门从网络信息内容执法加快向网络安全、数据安全、个人信息保护等领域执法拓展。

http://hn.news.cn/2022-11/19/c_1129141987.htm

7、俄黑客组织窃取 5000 万个用户密码

11 月 24 日消息，根据 Group-IB 公司报告，研究人员分

析发现至少 34 个不同的俄罗斯黑客组织使用信息窃取恶意软件在 2022 年 1 月至 7 月期间，从超过 89.6 万个用户处累计窃取了 5035 万账户密码。窃取的凭证信息包括加密货币钱包、Steam、Roblox、Amazon、PayPal 账户、以及支付卡记录。

Group-IB 分析发现，攻击活动的目标设计 111 个国家和地区，其中大多数的受害者位于美国、德国、印尼、巴西、印度。被盗凭证用于加密货币钱包、Steam、Roblox、亚马逊和 PayPal 账户以及支付卡记录，迄今为止被盗数据价值接近 600 万美元。

https://www.bleepingcomputer.com/news/security/russian-cybergangs-stole-over-50-million-passwords-this-year/

8、自由亚洲电台遭黑客攻击，近 4000 人个人资料外泄

11 月 22 日，据外媒报道，美国政府赞助的新闻媒体自由亚洲电台宣布了一项影响近 4,000 人的漏洞——其泄露了大量个人信息，包括社会保险号码和护照号码，以及财务数据。

根据提交给缅因州总检察长的文件，黑客攻击发生在 6 月 17 日，并于 6 月 28 日被自由亚洲电台发现。至少有 3,779 人受到黑客攻击的影响，其中包括地址、驾照号码、健

康保险信息、医疗信息被盗，以及“有限的财务信息”。调查确定，未经授权的访问是由于利用服务提供商的漏洞造成的，目前没有证据表明信息被滥用。

https://therecord.media/personal-data-of-nearly-4000-people-leaked-in-hack-of-radio-free-asia/?web_view=true

9、医疗软件公司暴露易受攻击的儿童敏感数据

11 月 23 日，据外媒报道，安全研究人员发现了一个未受保护的数据库，其中包含 16,000 多条记录。更糟糕的是，配置错误的数据库包含数千名儿童的敏感个人身份信息(PII)。

据调查，配置错误的数据库包含高度敏感的 PII，包括父母和孩子的姓名、出生日期、患者 ID 号、实际地址、特殊需要、就读学校、医疗诊断和社会/行为问题的历史。此类信息应该只供医学专家访问，但可以通过错误配置的 IP（指示主机域、登录门户和数据位置）公开访问。

此类敏感的健康记录泄露会带来一系列风险，并可能危及儿童及其家人的安全。暴露的数据可用于医疗勒索或网络钓鱼、社会工程诈骗，甚至可能导致数据加密的勒索软件攻击。

https://www.hackread.com/medical-software-expose-child-

data/?web_view=true

10、波多黎各的 DCH 医院遭到勒索攻击影响约 120 万名患者

11 月 22 日称，波多黎各的医生中心医院（DCH）遭到新勒索团伙 Project Relic 的攻击。攻击者已公开其窃取的 211 GB 文件中的 114 MB 数据，样本数据包括了医院系统的内部文件，关于员工的文件以及涉及病人医疗信息的文件等。DCH 在 11 月 9 日通知 HHS，有 1195220 名患者受到此次事件的影响。据 BlackPoint 称，Project Relic 勒索软件是用 Go 语言开发的，但用于安装恶意软件和窃取数据的方法仍然未知。

https://www.databreaches.net/doctors-center-hospital-reports-1-2-million-patients-affected-by-ransomware-attack/

11、花拉公园医院因泄露患者的医疗信息被罚款 58000 新元

据媒体 11 月 21 日称，花拉公园医院因泄露近 2000 人的医疗信息被罚款 58000 新元。泄漏事件发生在 2018 年 3 月 8 日到 2019 年 10 月 25 日，医院在 2019 年 10 月收到投诉后，于 2020 年 7 月向通报了这一事件。据悉，共有 9271 封邮件从两名医院员工的 Office 365 工作邮件帐户中自动转发

到第三方电子邮件地址，泄露信息涉及患者姓名、性别、身份证号码、护照详细信息、联系电话和医疗信息等。

https://www.databreaches.net/farrer-park-hospital-fined-s58000-over-data-breach-affecting-medical-information-of-2000-people/

12、印度坎努尔大学的官方网站泄露 3 万多学生的信息

11 月 21 日报道称，科钦的一家安全机构发现，印度坎努尔大学 2018 年至 2022 年注册的 3 万多名学生的信息被发布在一个黑客论坛上。根据初步推测，此次泄露事件是由于大学官方网站的技术故障导致的。泄露数据涉及学生的姓名、Aadhaar 号码、照片和电话号码等。目前，坎努尔大学已就此事采取行动，并决定从其数据库中删除 2018 年至 2022 年的所有数据。

https://english.mathrubhumi.com/news/kerala/personal-information-of-over-30-000-kannur-university-students-leaked-1.8066818

《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/