全球数据安全观察

总第 82 期 2022 年第 10 期

（2022.03.14-2022.03.20）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、国务院政府工作报告：强化网络安全、数据安全和个人信息保护

国务院总理李克强在十三届全国人大五次会议中的政府工作报告中提到，强化网络安全、**数据安全和个人信息保护**。这是自 2021 年政府工作报告以来，再次对数据安全和个人信息保护的强调。

报告还强调了促进数字经济发展。加强数字中国建设整体布局。建设数字信息基础设施，推进 5G 规模化应用，促进产业数字化转型，发展智慧城市、数字乡村。加快发展工业互联网，培育壮大集成电路、人工智能等数字产业，提升关键软硬件技术创新和供给能力。完善数字经济治理，释放数据要素潜力，更好赋能经济发展、丰富人民生活。加强数字政府建设，推动政务数据共享。创新发展服务贸易、数字贸易。——要统筹发展和安全，就是要在这些重点工作推动的过程中，将《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等合规要求细化落地，做好网络安全和数据安全保障。

https://mp.weixin.qq.com/s/xMEzrC2Hp19tJdAahaW3uA

2、国家网信办《未成年人网络保护条例（征求意见稿）》再次公开征求意见

3 月 14 日，国家互联网信息办公室会同司法部根据《未成年人保护法》《个人信息保护法》等法律，对《未成年人网络保护条例（征求意见稿）》进行了起草修改，并再次向社会公众公开征求意见。此次《条例》草案共七章六十七条，内容上较 2016 年第一次草案内容扩充将近一倍，就**未成年人信息保护**、防止未成年人沉迷网络、消费管理、禁止网络欺凌等方面作出规定，并表示严禁任何组织和个人以侵害未成年人身心健康的方式干预未成年人沉迷网络、侵犯未成年人合法权益。

2016 年的草案中，关于未成年人个人信息保护的规定较少，主要聚焦于企业应合理收集未成年人个人信息、应针对未成年人个人信息制定收集规则、赋予未成年人用户及其监护人撤回同意的权利等方面。但本次草案针对未成年人个人信息保护设立了专章，从**信息的收集、处理、使用、保护**等方面进一步细化，与《个人信息保护法》形成呼应，填补了部分制度空白。

https://mp.weixin.qq.com/s/3OhsAwb9MLmybx-prt9kFA

3、银保监：今年将开展银行业保险业个人信息保护专项整治

3 月 15 日，第 281 场银行业保险业例行新闻发布会在北京召开，主题为“银行业保险业深入推进金融消费者保护”专场新闻发布会。

银保监会消保局局长郭武平提出，2022 年银保监会将继续践行以人民为中心的指导思想，加大监管力度，重点开展银行业保险业**个人信息保护**专项整治。现在各行各业都把信息作为竞争的核心，同时个人信息保护也存在很多问题和漏洞，应推动银行业保险业切实落实《个人信息保护法》，**提升个人信息使用的规范性，保护消费者信息安全权**。

银保监会指出，一些金融机构、互联网平台在开展相关业务或合作业务时，对消费者个人信息保护不到位，比如以默认同意、概括授权等方式获取授权；未经消费者同意或违背消费者意愿将个人信息用于信用卡业务、消费信贷业务以外的用途；不当获取消费者外部信息等。以上过度收集或使用消费者个人信息的行为，侵害消费者个人信息安全权。

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

4、国家网信办：将开展算法治理行动 督促整改大数据杀熟

3 月 17 日，国家网信办网络管理技术局局长于永河在国务院新闻办新闻发布会上答南都记者问时表示，将严厉打击

算法违法违规行为，督促整改算法不合理应用带来的“信息茧房”“算法歧视”“大数据杀熟”等影响网民生产生活的问题。于永河表示，国家网信办将于近期启动 2022 年“清朗·算法综合治理”专项行动，时间将持续到今年年底。

该行动深入检查各类算法应用的情况，针对违反《管理规定》的现象和行为，依法依规进行惩治和处罚，严厉打击算法违法违规行为；同时也督促企业开展算法备案，履行好主体责任。督促整改算法不合理应用带来的“信息茧房”“算法歧视”“大数据杀熟”等影响网民生产生活的问题，切实维护好网民合法权益。

https://mp.weixin.qq.com/s/RVfP4gHY8DCyXoPFrkWz6w

5、广西加快数据要素市场化改革实施方案

3 月 18 日，广西壮族自治区大数据发展局发布关于《广西加快数据要素市场化改革实施方案》。方案的主要目标是：建立全区统一开放的数据要素市场；构建两层数据要素市场结构，发挥行政机制和市场机制比较优势，激发各类供需主体活力。一层市场以政府行政机制为主，通过管、建、运适度分离，建设公共数据运营平台，为数据要素流通提供保障；二层市场以市场竞争机制为主，建设各类数据交易场所，规范数据进场交易；建设三类数据要素市场化平台。围绕**数据**

要素资源化、资产化、资本化，建设数据要素集聚平台、运营平台和交易平台，保障数据要素生产、分配、流通等各环节循环畅通；构建数据要素市场供给、流通、应用、监管“四位一体”体系，在各个行业领域探索数据要素赋能场景，释放数据要素生产力潜能。主要任务有四点：一、构建多元发展的**数据要素市场供给体系**；二、建立开放有序的**数据要素市场流通体系**；三、构建高效协同的**数据要素市场应用体系**；四、建立科学完备的**数据要素监管体系**。

https://mp.weixin.qq.com/s/HiE418ZdK1-r25B80N1n3Q

6、信安标委印发 2022 年度工作要点，研制重要数据保护、数据安全风险评估等关键标准

3 月 15 日，信安标委印发《全国信息安全标准化技术委员会 2022 年度工作要点》的通知。文件指出，信安标委将加快研制急需关键标准，着力提升标准实施应用效果，努力推动网络安全国家标准由数量规模型向质量效益型转变。2022 年工作要点如下：(一)聚焦中心工作，加快研制网络安全急需重点标准；(二)加强前瞻研究，做好网络安全标准规划工作；(三)创新形式举措，提升网络安全标准宣传效果；(四)拓展全球视野，促进国内国际标准协同发展；(五)强化能力建设，提升标准高质量发展保障能力。

https://mp.weixin.qq.com/s/_gfrbVh_L6ZokxrOi7qvFg

7、广东省：建设省数据交易场所和粤港澳大湾区大数据中心

近日，广东省印发广东省数字政府改革建设 2022 年工作要点。拟全面推进**数据要素市场化配置改革**，进一步健全公共数据管理和运营体系，完善数据交易流通平台和机制，加强数据要素相关标准和技术研究，探索构建个人和法人数字空间，力争在年内取得新突破，推动数字经济创新发展。其中，拟促进数据交易流通。依托现有交易场所建设省数据交易场所，搭建**数据交易平台**。推动**数据经纪人**、“数据海关”试点。支持深圳市设立数据交易市场或依托现有交易场所开展数据交易。探索运用区块链、隐私计算等新技术**强化数据安全防护**。建设粤港澳大湾区大数据中心，健全大湾区数据基础设施体系。

https://mp.weixin.qq.com/s/4aJ0h2QeO7fytgDc-EZSuA

8、法国数据保护机构 CNIL 发布 2022-2024 年战略规划

法国数据保护机构 CNIL 近期发布了 2022-2024 年战略计划，专注于以下三个关键主题：鼓励控制和尊重个人权利、将欧盟 GDPR 作为一项值得信赖的资产进行宣传，以及优先针对“高风险隐私问题的监管行动”。CNIL 主席玛丽-洛尔·丹

尼斯表示，该计划“应该使 CNIL 能够以灵活的方式与公民、公司、协会和当局一起行动，从而建立一个值得信赖的数字社会。”

https://mp.weixin.qq.com/s/oH2SUrUe-W1-7pDM2VUHjA

技术、产品与市场

1、IDC：2025 年中国网络安全市场规模将超 214 亿美元

IDC 数据显示，2021 年中国网络安全相关支出有望达到 102.6 亿美元。预计到 2025 年，中国网络安全支出规模将达 214.6 亿美元。在 2021-2025 的五年预测期内，中国网络安全相关支出将以 20.5%的年复合增长率增长，增速位列全球第一。

相较于增速放缓的全球网络安全服务市场，中国安全服务市场将以近全球两倍的五年复合增长率快速增长。IDC 预测，在 2021-2025 的五年预测期内，中国网络安全服务市场年复合增长率将达到 20.8%，到 2025 年，其市场规模预计将超过 61.1 亿美元。其中，**安全咨询服务（Consulting Services）在未来五年仍为最大的服务子市场**，到 **2025** 年，咨询服务市场的规模将达到 **24.6 亿美元**。与此同时，在安全运营需求不断爆发的大背景下，中国托管安全服务（Managed Security

Services）市场发展势头强劲，五年复合增长率预计达到31.9%。

https://www.secrss.com/articles/40362

2、云安全联盟发布《隐私科技白皮书》

近日，云安全联盟发布了《隐私科技白皮书》(以下简称“白皮书”)。白皮书结合当前我国隐私科技发展现状及产业发展环境，以数据为基准，对隐私科技发展趋势作出预测，为行业提供参考。

白皮书从隐私合规、数据安全、数据可用的维度出发，开创性的提出了“隐私科 技”的概念，详细描述了其定义、发展历程、技术以及应用场景，分析了全球以及中国的隐私科技产业环境，同时深入浅出的描绘了隐私科技的发展趋势，值得大家参考。

其中，白皮书提到“隐私科技”概述。隐私科技是一系列技术与解决方案的集合，它包含了如隐私计算，隐私增强技术，数据安全技术，数据及隐私合规科技等诸多技术领域范畴。隐私科技通过数字化手段解决组织在隐私保护工作中面临的痛点，在提升数据流通与共享能力的基础上确保数据安全与个人隐私得到有效的保护。

https://mp.weixin.qq.com/s/72PoBULp-hCUXh2TXbegFw

3、360 入选 Gartner 中国安全运营标杆厂商

近日，国际权威 IT 咨询机构 Gartner 对外发布《中国安全运营代表厂商名录》，**360 政企安全集团**凭借在安全运营领域过硬的产品技术实力和卓越的市场表现入选 Gartner 中国安全运营标杆厂商，并覆盖安全运营市场中的四个细分领域（SIEM、SOAR、TI、VA）。**这是继 2021 年 360 凭借重庆合川区安全运营中心入选 IDC 智慧城市安全运营技术服务提供商后，其安全运营能力再次获得国际权威咨询机构的认可。**

作为全球权威的 IT 研究与顾问咨询公司，Gartner 中国通过分析安全厂商产品的综合实力评估各领域的标杆安全厂商，旨在为寻求安全工具的需求方提供价值性的参考信息。此次，360 政企安全集团旗下三款本地安全大脑家族产品：360 态势感知平台、360 安全分析响应平台、本地安全大脑入选 SIEM、SOAR、TI，360 漏洞管理平台产品入选 VA，体现了 Gartner 对 360 政企安全集团在安全运营领域突出的专业能力和成熟度的认可与肯定。

https://www.anquanke.com/post/id/270429

4、从北约量子安全通信测试看后量子密码技术发展

3 月 3 日，北约网络安全中心(NCSC)完成量子安全通信

测试。此次测试使用其专门的虚拟专用网络（VPN）之一测试了“安全通信流”，并将其技术描述为“混合后量子 VPN”，它将传统加密算法与那些被认为是“量子安全”的算法混合在一起。此次测试的成功，一方面表明以量子计算为代表的计算能力飞跃发展，量子计算变得越来越便宜、可扩展和实用，另一方面密码算法体系如何抵抗量子计算攻击成为重要而紧迫的问题，基于新型数学难题的后量子密码技术开始担负起抵御量子计算挑战的重任。

https://mp.weixin.qq.com/s/WcXhxiLQT3NY8jzdmTSZ2Q

5、产业观察：网络安全产业的八维研判

正在进行的俄乌冲突中，网络空间成为双方博弈的另一战场，甚至直接影响到战争的走向。实际上，网络安全对政治、经济、民生、科技，以及各行业的发展正产生日益重大的影响与相互作用。同时，政策法规、产业格局、新兴领域和投融资等关键因素也影响网络安全产业发展。

1) 新政治安全: 网络安全成为大国政治建设与博弈的焦点;
2) 新经济安全：数字化产业需要网络安全同步;
3) 新科技安全：科技创新应用需要网络安全先行;
4) 新政策法规：从政策驱动转向法律驱动，数据安全成

为焦点；

5) 新产业格局：国际趋势与国家特色并存，我国政企市场特点显著；
6) 新兴热门领域：网络安全产业转型，新兴领域发展迅速；
7) 新投融资热点：资本市场高度看好，二级市场认知有待提升；
8) 新产业阶段：“十四五”是网络安全产业发展的战略机遇期。

https://mp.weixin.qq.com/s/1ZNUGNshnbnYvrgVQZ3uBQ

6、这四种类型的勒索软件占报告事件的近四分之三

根据网络安全公司 Intel 471 的分析，到 2021 年底，四种恶意软件菌株总共占所有攻击的近 70%。最普遍的勒索软件威胁是 LockBit 2.0，占所有报告事件的 29.7%，其近期受害者包括埃森哲和法国司法部。几乎五分之一的报告事件涉及 Conti 勒索软件，该勒索软件在过去一年中以多起事件而闻名，其中包括对爱尔兰卫生健康服务署的攻击。PYSA 和 Hive 两款勒索软件各占报告的勒索软件攻击的十分之一。

https://www.zdnet.com/article/these-four-types-of-ransomware-make-up-nearly-three-quarters-of-reported-incidents/

业界观点

1、陈晓红：加强我国跨境数据流动监管

数字经济正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。全国政协委员陈晓红认为，**亟需通过制度创新增强跨境数据流动监管，打造全球数据要素汇聚高地，营造全球开放的数字经济营商环境**。

为此，陈晓红提出五点建议：

一是完善跨境数据流动管辖法律法规体系。构建跨境数据流动监管的国际互信机制，开展数据出境安全评估、数据保护能力认证、标准合同条款、“白名单”等机制建设。同时，要健全数据出境安全评估配套措施。

二是推进数据跨境流动安全保障能力建设。要加强数据安全风险评估、追踪溯源、监测预警等技术能力建设，支持数据跨境流动安全保障技术研发。同时，建立数据全生命周期安全保护责任制度。

三是强化跨境数据流动安全的内审机制建设。加强数据安全保护法治教育，提高企业敏感数据合规管理意识；加强对数据输出方的监管，加强数据安全风险监测和评估，建立数据泄露等安全事件的应急响应机制；建立数据接收方资格审查等监管机制。

四是积极推进数据跨境流动中国治理方案。要积极加入APEC框架下的GDPR体系建设；主动参与数据跨境流动的多边或双边协定谈判；充分利用“一带一路”建设契机，在数字经济治理上及时提出中国方案，发出中国声音。

五是建议构建统合跨境数据监管职权与技术资源的新机制。对敏感个人数据、商业数据、国家安全敏感数据及关键基础设施信息建立分级分类管理制度；要明确包括第三方数据交易机构、数据源机构等在内的数据交易主体的资质和权责，制定跨境数据交易规则等。

https://economy.gmw.cn/2022-03/10/content_35576136.htm

2、武超则：解决数据安全问题需要体系化的能力

武超则在他的前沿课·数字产业10讲中提到，今天的数据安全和过去相比，最大的不同是：第一，数据是流动的，数据随时随地产生、随时随地存在、随时随地被使用，所有的环节都要考虑数据保护。第二，数据安全的保护，也不再只是保护存储在某个地方的静态数据，而变成了一种体系化的、全流程的数据保护。

这给整个数据安全行业，带来了巨大的变化。最直接的就是，**数据安全厂商不再可能单靠单项技术来解决数据安全问题，而必须要有体系化的能力**，要能拿出整体的数据安全

解决方案。这种体系化的能力体现在两个方面：

第一，在规划层面，就要有体系化的能力。过去做数据安全，是外挂式的，就是等用户把所有系统都建好之后，再外接一个安全产品。现在不行了，因为要考虑到数据在各个业务、各个应用之间流转，所以在规划信息化方案的时候，就要做安全同步，把安全产品嵌入到信息化中去。这就要求，头部的数据安全公司一定要有整体的规划咨询能力。

第二，数据安全厂商的产品，也要有体系化能力。数据安全厂商要能提供一套完整的解决方案，在数据流转的每个环节，都有相应的防护能力。比如，当数据在内存当中的时候，怎样防止内存中的数据泄露；当数据存储在数据库的时候，怎样保证数据库不被篡改；当数据在网络端流转的时候，怎样防止数据被截取等等。

http://www.xiaomiio.com/news/13876.html

3、卫士通谈 315 数据安全问题：引入政治可靠、技术过硬、值得信赖的第三方数据安全合规服务方势在必行

2019-2022，连续四年都曝出消费者个人信息被违法违规收集使用的情况，我们不禁要问，难道保障个人信息安全真的这么难吗？

卫士通指出，很多互联网公司也在积极响应国家政策和

法律要求，加强了关于个人信息安全合规的整改，但过程中依然存在一些问题，也面临一些难题:

（1）在处理信息时落实“最小方式、最小范围、最短时间”的原则依然不到位。

（2）对敏感个人信息处理的重视不足。

（3）对第三方产品和服务的管理不足。

（4）自我监管不足。

（5）个人信息权利保障不足。

卫士通分析表示，数据安全合规包括个人信息安全合规，数据安全合规与信息系统、业务、场景等紧密关联，对数据安全合规进行深入地审计需要基于日志等证据数据，进行关联分析、综合评判，这就对审计机构提出了较高的要求。

外部审计比较难深入业务、了解细节，可能存在审计不充分的问题，缺少刻画出数据流转、数据流向、全生命周期关联活动的技术证据，而且评估、审计等缺乏一定的时效性，监管存在滞后。

对此，卫士通认为数据作为一种“生产要素”，就确立了其在新时代中国特色社会主义经济中的地位。个人信息在《民法典》中明确为一项人格权益，面向数据安全合规特别是个人信息安全合规，引入政治可靠、技术过硬、值得信赖的第三方数据安全合规服务方势在必行。

https://mp.weixin.qq.com/s/vJNeZ1wrUZkig1kyY6GCOA

4、多位专家建议 App 用户协议清单制

在下载 APP 使用，点击“我已阅读并同意用户协议和隐私政策”这个常规操作中，武汉大学网络治理研究院副院长袁康所在的联合调研组去年对 1036 人进行调查访谈的结果显示，77.8%的用户在安装 App 时“很少或从未”阅读过隐私协议，69.69%的用户会忽略 App 隐私协议的更新提示。

“用户协议和隐私政策写满了大量冗杂信息，专业人士都直呼头疼，更别提普通消费者了。”袁康认为，“少有人读”反映出相关协议仍“形同虚设”，达不到保障用户知情权的初衷。

近年来，App 用户协议和隐私政策在治理中逐步完善。不过，部分 App 协议仍然存在着如不同意则不能用、先斩后奏、一次同意则次次同意、个人信息转送第三方等陷阱。

对此，左晓栋等多位专家认为，一些 App 用户协议和隐私政策有通过晦涩难懂的文字浑水摸鱼的嫌疑，呼吁通过清单制简洁明了地列出消费者需要了解的内容，降低阅读门槛。

天津财经大学商学院互联网信息与用户行为研究中心主任陈旭辉、袁康等呼吁，用户协议普遍内容繁杂，有必要从用户便捷阅读需要出发，将与用户关联的重要部分在协议

前面突出显示，类似上市公司年报和学术论文摘要，方便用户了解隐私协议核心内容。同时，“相关协议还要进一步明确‘必需信息’‘第三方’等核心要素的范围，不能含糊地概括为‘可能向第三方披露’。在分享用户信息的时候，也要将敏感的个人信息匿名化处理。”袁康说。

陈旭辉认为，监管部门可抓住手机应用市场这个“关键少数”，明确其上架违规 App 的相应法律责任，推动其从上架 App 的源头上做好把控工作。

http://tj.news.cn/news/2022-03/15/c_1128470903.htm

5、河南省消费者协会发布个人信息保护情况专项调查结果

3 月 14 日，河南省消费者协会发布了个人信息保护情况专项调查结果。本次调查样本覆盖河南 18 个省辖市，共完成 3017 个样本。本次调查主要结果如下:

一、有 52.2%的消费者表示知道《中华人民共和国个人信息保护法》已通过并实施。

二、21.8%的消费者对于个人信息保护现状表示不满意 64.9%的消费者表示比较满意或基本满意，仅 9.0%的消费者表示对个人信息保护现状很满意。

三、关于信息泄露的原因，66.5%的消费者认为信息的非法售卖是主要原因，52.9%的消费者认为随意丢弃快递单号、

银行账单等也是个人隐私信息泄露的主要原因。

四、如果发生消费者个人信息泄露并造成影响，选择报警的消费者最多，占比 59.5%；其次是向国家网信办举报，占比 37.3%；36.2%的消费者会寻找和联系信息泄露源，要求其依法依规采取消除影响、经济赔偿等措施。

五、超过半数的消费者遇到过个人信息被过度收集的情况。

六、消费者遇到个人信息被过度收集的情况主要存在于以下几方面：

1）各类社交生活类 App 过度收集个人信息，被消费者认为存在强制要求授权、窃取个人信息的风险。

2）招聘求职、教育机构等平台，消费者对这些平台过度收集家庭成员、住址、收入状况等个人信息表示担忧。

3）房产中介、银行、保险公司等组织机构，121 名消费者提到房产中介，76 名消费者提到银行，42 名消费者提到保险公司。消费者表示机构过度收集个人信息，导致经常收到办卡、卖房、卖保险等信息骚扰。

七、63.2%的消费者认为非常有必要进一步加强当前社会在个人信息方面的保护。

对此，省消费者协会从监管、消费者层面提出具体建议。

在监管层面，通过设立专门监管机构，加强监督管理，

协调有关部门加强个人信息保护工作，并建立统一的制度规范；加快完善法律制度，对侵犯个人隐私和个人信息安全的行为进行严厉打击和惩处。

在消费者层面，保护个人信息，记好“四个要”：一要重视自己的个人信息保护，认真学习个人信息保护法。二要养成“非必要不提供”的习惯。三要保护好自己的个人信息。不轻易在网上“晒”与个人信息相关的内容与资料，对于一些容易造成自己信息泄露的资料，如快递、外卖订单，应及时妥善处理。四要主动用法律武器维护自身权益。

https://dsj.henan.gov.cn/2022/03-15/2414169.html

数据安全事件

1、Meta 因数据泄露违反隐私规则，被欧盟罚款 1700 万欧元

2022 年 3 月 16 日消息，Meta 因 2018 年未能阻止 Facebook 平台上的一系列数据泄露，违反了欧盟的隐私规则，被罚款 1700 万欧元（合 1900 万美元）。

Meta 的主要欧盟隐私监管机构爱尔兰数据保护委员会表示，它发现 Facebook“未能采取适当的技术和组织措施”。2018 年，Facebook 成为欧盟《通用数据保护条例》的首个重大测试案例，爱尔兰监管机构宣布对一起影响 5000 多万个账户的违规事件展开调查。调查于当年 12 月开始，调查对象是 Facebook 发出的 12 条违规通知，其中一些由一个软件漏洞引起，该漏洞让外部开发者获得了数百万用户的照片。

https://baijiahao.baidu.com/s?id=1727411877760316913&wfr=spider&for=pc

2、前 CafePress 老板因掩盖数据泄露被罚款 500,000 美元

2022 年 3 月 17 日，据外媒报道，CafePress 的前任老板因一连串的安全故障和数据泄露被罚款 500,000 美元。CafePress 是美国一个网络平台，提供按需印刷产品，包括服

装、家居装饰和厨具。而这需要卖家和买家提供关键的财务信息才能运营，因此，CafePress 需要安全地管理这些信息并在处理交易时考虑到安全性。

然而，调查显示，该平台缺乏“合理的安全措施”来防止数据泄露，并掩盖重大违规行为。CafePress 保留用户数据的时间超过了必要的时间，以明文形式存储了包括社会安全号码和密码重置答案在内的个人身份信息 (PII)，并且没有针对已知的系统漏洞进行修补。

https://www.zdnet.com/article/cafepress-fined-500-million-for-shoddy-security-covering-up-data-breach/

3、丰田供应链又被黑客盯上：日本电装公司遭勒索软件攻击

2022 年 3 月 18 日报道，日本三井物产安全方向公司消息称，当地时间 3 月 13 日下午，一个自称名为“潘多拉”（Pandora）的网络犯罪组织在暗网上发布声明称，该组织窃取了日本电装公司（Denso）的机密数据，并声称将公布这些数据。据悉，电装公司是一家总部位于日本爱知县的丰田集团下属大型汽车零部件厂家。

“潘多拉”发布声明称，该组织盗取的数据包括采购订单、电子邮件、设计图纸等，总计超过 15.7 万件，数据量达 1.4TB。

https://www.secrss.com/articles/40461

4、俄罗斯管道巨头 Transneft 遭攻击，79GB 数据泄露

2022 年 3 月 18 日报道，俄乌冲突进入第 3 周，一些非常规行为者继续针对俄罗斯国家支持的企业发起攻击，进行一连串的黑客攻击和数据泄露。而由俄罗斯国家控制的石油管道巨头 Transneft 无疑成为了重点攻击对象。

周四，泄密托管网站 Distributed Denial of Secrets 发布了一个 79GB 的电子邮件链接，这些电子邮件来自 Transneft 的研发部门 Omega 公司。泄露的电子邮件似乎包含了公司员工的多个电子邮件账户的内容，不仅包括电子邮件信息，还包括包含发票和产品发货细节的文件附件，以及显示服务器机架和其他设备配置的图像文件。

https://www.cnbeta.com/articles/tech/1248347.htm

5、南非顶级征信机构 TransUnion 遭遇数据泄露，黑客索要 1500 万美元赎金

2022 年 3 月 18 日，据外媒报道，南非的一家顶级征信机构遭遇数据泄露，黑客索要约 1500 万美元的赎金。“犯罪第三方通过滥用授权客户的凭据获得了对 TransUnion South Africa 服务器的访问权限。”该公司表示，赎金要求“不会支付”。一个自称为 N4aughtysecTU 的组织声称为该事件

负责，并表示“我们拥有超过 4TB 的所有客户信息。这些信息涵盖了 200 多家公司”。

https://www.cyberscoop.com/south-africa-transunion-data-breach/

6、“匿名者”入侵俄罗斯最大石油公司，窃取 20TB 数据

2022 年 3 月 16 日报道，近日，“匿名者”声称入侵了俄罗斯能源巨头 Rosneft 德国子公司的系统，并窃取了 20TB 的数据。这一入侵的消息也得到了德国联邦信息安全局 BSI 的证实，BSI 表示支持调查安全漏洞，且已经向石油行业的其他利益相关者发出了安全警告。

https://mp.weixin.qq.com/s/HpQ_-FOYnA7gGkqjAq6xzg

7、2,113 个移动应用程序因云配置错误而暴露用户数据

2022 年 3 月 16 日，据安全供应商 Check Point 称，由于后端云数据库配置错误，具有数千万下载量的移动应用程序正在泄露敏感的用户数据。

“开发人员经常手动更改安全规则来运行测试，如果在将应用程序发布到生产环境之前未锁定安全配置，将使数据库对任何访问它的人开放，因此容易对数据库进行读写。”在整个研究过程中，Check Point 共发现了 2113 个移动应用

程序，它们的 Firebase 后端由于配置错误而暴露，包括：一个南美电子商务应用程序，下载量超过 1000 万次，泄露了 API 网关凭据和 API 密钥；一个标志设计应用程序，下载量也超过 1000 万次，暴露了 130,000 个用户名、电子邮件和密码；一个社交音频平台，下载量超过 500 万次，暴露了银行详细信息、位置、电话号码和聊天消息等等。

https://www.infosecurity-magazine.com/news/thousands-mobile-apps-expose-data/?&web_view=true

8、因恶意软件攻击，100 万德州人的牙科保健数据遭受泄露

2022 年 3 月 18 日报道，多达 1,026,820 名德克萨斯人可能受到涉及大型牙科保健提供商的大规模数据泄露的影响。该违规行为于周四发布在该州的网站上，这是自新的德克萨斯州法律于 9 月生效以来向德州总检察长报告的最大违规事件。迄今为止，没有证据表明信息已被滥用，可能暴露或获取的信息类型中包含社会安全号码、驾驶执照号码、健康保险信息和财务信息。

https://dfw.cbslocal.com/2022/03/18/million-texans-impacted-dental-care-data-breach/?&web_view=true

9、美国 SDCA 遭到入侵，近 30 万个心脏病患者的信息暴露

2022 年 3 月 15 日，据外媒报道，美国南丹佛心脏病协会(SDCA) 遭到入侵，约 287652 个患者的信息暴露。SDCA 表示，他们于 1 月 4 日在计算机系统中发现了异常活动，之后立即启动了事件响应流程。此次泄露的信息包括患者姓名、出生日期、社会安全号码、驾驶证号码、患者帐号、健康保险信息和临床信息等。SDCA 已将此次泄露事件通知受影响的用户，并将为其提供免费的信用监控和身份保护服务。

https://www.infosecurity-magazine.com/news/heart-patients-data-exposed/