全球数据安全观察

总第 131 期 2023 年第 12 期

(2023.03.27-2023.04.02)

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、《关于开展网络安全服务认证工作的实施意见》

3 月 28 日，市场监管总局、中央网络安全和信息化委员会办公室、工业和信息化部、公安部四部门发布《关于开展网络安全服务认证工作的实施意见》。《意见》从网络安全服务认证机构、通过认证的网络安全服务机构、网络运营者以及监管部门四类主体的维度，就开展国家统一推行的网络安全服务认证工作提出九点意见，对《中华人民共和国网络安全法》第十七条中国家鼓励开展网络安全认证、检测和风险评估等安全服务进行落实。

http://www.gov.cn/zhengce/zhengceku/2023-04/02/content_5749741.htm

2、文旅部：加强旅游者个人敏感信息保护

3 月 27 日，文化和旅游部发布《关于推动在线旅游市场高质量发展的意见》，围绕市场环境、市场秩序、行业发展等方面提出要求。其中，《意见》提出要保障旅游者合法权益，包括：加强旅游者个人敏感信息保护，防止超出合理经营需要收集旅游者个人信息，采取切实措施避免大数据杀熟、虚假宣传、虚假预订等侵害旅游者权益行为。

http://www.gov.cn/zhengce/zhengceku/2023-03/28/content_5748755.htm

3、《“河南链”建设实施方案（2023—2025年）》印发

3月28日，河南省人民政府办公厅印发《“河南链”建设实施方案（2023—2025年）》，从总体架构、公共基础平台架构、与其他业务系统的关系方面对“河南链”进行了架构设计，并提出了七项重要任务：构建“河南链”云链融合网络、建设“河南链”数据共享链、推动“河南链”示范应用、开展“河南链”区域试点、建立“河南链”标准体系、助力数据要素市场发展、培育区块链产业生态。

https://www.henan.gov.cn/2023/03-28/2715211.html

4、首项数据资源规划标准正式发布

近日，《信息技术 大数据 数据资源规划》（GB/T 42450-2023）经市场监管总局（标准委）批准发布，将于2023年10月1日起正式实施。该标准以组织确定的业务规划与目标为输入，系统性设计开展数据资源各要素的规划、描述，并基于已有法律、规章、标准等规则，提出规范性要求。

https://mp.weixin.qq.com/s/Tn4JGq90GDw8Ik3kT3VBDw

5、首个“数据资产价值与收益分配评价模型”标准发布

3 月 28 日下午，全国首个“数据资产价值与收益分配评价模型”标准（以下简称“数据资产评价标准”）在青岛发布。数据资产评价标准从数据运营过程中的数据资产价值评价与收益分配评价入手，根据数据在运营过程中的使用与收益情况，量化数据质量、数据应用、变现量和收益分配比例，进而对数据资产的价值与收益分配进行评价。根据此标准开发设计的评价模型，对数据流通过程中产生的价值数据以可追溯且不可篡改的形式记录在区块链上，在上链数据可信的基础上进行量化计算、价值评价，并将评价结果作为数据资产评估的依据，为数据资产融资和入表做准备。

https://mp.weixin.qq.com/s/umFEdCVFpjajPSvcugby1w

技术、产品与市场

1、美国军方正在加速实施零信任

据 Inforisktoday 消息，在五角大楼举办的一场研讨会中，五角大楼一位高级技术官员 3 月 29 日强调，美国国防部将零信任作为保护军事网络的途径。

国防部首席信息安全官 Sherman 在参议院武装部队网络安全小组委员会上说：“承诺到 2027 年在整个国防部实施零信任，鉴于我们面临的地缘政治威胁，这是一个雄心勃勃但又至关重要的里程碑。”

军方网络提供商、国防信息系统局一年来一直在通过一个名为 Thunderdome 的项目实施零信任，并且已经取得了初步的成果。

https://www.freebuf.com/news/362244.html

2、微软推出 Security Copilot：内置 GPT-4，自动抵御 65 万亿个网络安全威胁

北美时间 3 月 28 日，微软召开首届“Microsoft Secure”大会，并宣布推出网络安全产品——Microsoft Security Copilot。

据悉，Security Copilot 将目前最强大语言模型 GPT-4 内

置在产品中，并与微软拥有 65 万亿个网络安全威胁的安全模型库相结合使用，为企业、个人用户提供网络安全、恶意代码防护、隐私合规监控等生成式自动化 AI 服务。

多数传统网络安全软件经常需要数小时甚至数天才能对安全事件做出反应，而企业、个人用户在 Security Copilot 帮助下，可实现“分钟级”安全事件响应、评估、防御，以保证数据资产安全。

https://mp.weixin.qq.com/s/fgU4eaaF7NXSGU9nXd6TYg

3、隐私计算未来趋势：融合与提升，方案可落地

隐私计算是数据隐私保护的重要手段，在大数据时代越来越受到关注。**未来，隐私计算的发展趋势将是技术融合，即将多种技术进行整合，形成更加综合和灵活的隐私计算方案。**

在技术融合方面，多方安全计算、联邦学习和可信执行环境等技术将会相互协同，互相弥补优劣，提高隐私计算的效率和安全性。

在性能提升方面，未来的隐私计算趋势将是提升性能，通过优化硬件、算法和通信等方面的技术指标，以降低性能损耗，实现更高效的隐私计算。

在方案落地方面，隐私计算厂商需要根据用户的具体业

务需求，提供定制化的解决方案，包括技术方案、应用方案和商业模式等。为了实现方案的落地，隐私计算厂商需要与行业合作伙伴紧密合作，共同推动隐私计算技术在具体场景下的应用。同时，隐私计算厂商还需要提供全方位的技术支持和培训服务，帮助客户快速上手并应用隐私计算技术。

https://mp.weixin.qq.com/s/h4rtlio3Ao3RqjaQyVVe3w

4、IDC：2026 年中国数据量规模将达到 56.16ZB 年均复合增长率 CAGR 达到 24.9%

IDC 预测，2026 年中国数据量规模将达到 56.16ZB，年均复合增长率 CAGR 达到 24.9%，位居全球第一。数据作为数字经济时代的重要生产要素，其安全性、开放流通、价值挖掘引发的关注与热度不断攀升。利用隐私计算技术实现数据合法合规的共享与开放，在数据流动中挖掘数据价值并进行业务创新已经成为众多企业的重要战略及执行方向。

在数据使用需求与合规趋于严格的双重因素推动下，越来越多的企业开始尝试运用隐私计算技术解决数据流动共享问题。当前，在联合风控、联合营销、数据开放等场景，隐私计算的能力已经得到显现和印证。下一阶段，技术买家需要更加聚焦于如何让技术从试点走向大规模的业务应用，其中一套完整且合规的技术推行审批机制、充分吸纳同时掌

握业务和技术的双料人才、从数据中介向数据运营者转变等都将成为技术拓展并实现盈利的发展关键。

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

5、贵阳大数据交易所提出“SEED”罗盘模型培育和建设数据要素市场

近日，《数字经济》刊发文章，以全国首个大数据交易所——贵阳大数据交易所作为研究对象，基于其实践发展和创新探索，首次提出 SEED 罗盘模型培育和建设数据要素市场。S（System of rules，规则）指规则、标准、政策、法律；E（Exchange platform，平台）指可信可控可靠可溯的数据交易所；E（Ecosystem，生态）指数据产业生态，包括数据供给方、数据需求方、数据中介、监管方等全生命周期生态体系；D（Data，数据）指提供的各类型数据交易标的，分为公共数据、企业数据、个人数据。

https://mp.weixin.qq.com/s/YPZVyyKQ4DBtjCHUKBPoGQ

业界观点

1、国家发改委：推动有条件的地方和行业开展数据要素流通使用先行先试

4 月 3 日，国务院新闻办举行发布会上，国家发展和改革委员会创新和高技术发展司负责人孙伟介绍，近年来，国家发改委深入贯彻党中央、国务院决策部署，各地方、各部门持续推进数字经济发展，我国数字经济取得了举世瞩目的成就，数字基础设施实现了跨越式发展，数字产业创新能力加快提升，数字技术与实体经济融合提档加速，公共服务数字化深入推进。数字经济国际合作行稳致远，对经济社会发展的引领支撑作用日益凸显。

孙伟表示今年国家发改委将从六方面发力，不断做强做优做大我国的数字经济。

一是加强政策制度建设。加快构建“1+N”的数据要素基础制度体系，推动有条件的地方和行业开展数据要素流通使用先行先试，统筹构建多层次、多元化和场内场外相结合的数据要素市场体系。

二是适度超前部署数字基础设施建设。加快光纤网络扩容提速，5G 的商用部署和规模应用，深入实施“东数西算”工程，加快基础设施数字化、智能化的改造。

三是大力推动数字产业创新发展。培育一批具有核心竞争力的生态主导型企业，加快打造具有国际竞争力的数字产业集群，支持平台企业在引领发展、创造就业、国际竞争中大显身手。

四是加快深化产业数字化转型。强化各领域、各行业全方位、全链条数字化政策改造引领，提升“上云用数赋智”水平，提升新一代的信息技术与一二三产业融合发展，支持龙头企业、第三方服务企业带动中小企业加快转型的步伐。

五是持续提升数字公共服务水平。提高公共服务资源的数字化供给和网络化服务水平，持续加大适老化的智能化产品供给，运用数字技术为弱势群体增加便利，持续推进智慧城市和数字乡村融合发展。

六是不断深化数字经济国际合作。积极提出“中国倡议”，落实全球发展高层对话会数字经济领域成果。积极提供“中国方案”，推进加入《数字经济伙伴关系协定》，开展双多边数字经济治理合作，构建良好的国际环境。

http://finance.people.com.cn/n1/2023/0403/c1004-32656745.html

2、程啸：应当尽快制订个保法司法解释

自 2021 年 11 月 1 日《个人信息保护法》（下称《个保

法》）正式施行，目前已过去一年半的时间，但法院受理的个人信息保护纠纷案件的总体数量依然较少。

清华大学法学院副院长、教授、博士生导师程啸认为通过《个保法》司法解释对一些焦点、疑点与难点问题的科学系统规定，既可以为法院处理个人信息保护纠纷案件提供清晰准确的裁判规范，也能为律师、法务人员等实务人士提供指引，更能促进行政执法部门制定相应的规章和文件。他建议《个保法》的司法解释围绕**个人信息处理规则、个人信息权益的行使与救济、个人信息侵权责任**等三大问题作出清晰具体的规定。

建议一：个人信息处理规则需清晰具体

《个保法》第二章“个人信息处理规则”采用了 25 个条文，对个人信息处理的合法性根据、告知同意规则、多人处理个人信息的四种情形，以及公开个人信息与敏感个人信息的处理、国家机关处理个人信息等内容作出了系统的规定。个人信息处理规则对于行政执法和司法审判中判断个人信息处理活动是否为非法行为，以及是否侵害个人信息权益至关重要。

从实践来看，个人信息处理规则中有**“个人信息处理合法”的证明责任、“告知义务履行”的证明责任、“单独同意”的认定**等方面的问题需要明确。

建议二：解决个人信息权益行使与救济争议

个人信息权益是个人针对其个人信息享有的人格权益，《个保法》对于个人信息权益的内容专章作出了详细规定，明确了个人针对其个人信息处理享有知情权、决定权、查阅权、复制权、可携带权、更正权、补充权、删除权、解释说明权等。并且，《个保法》还专门规定，如果处理者拒绝个人行使权利的请求的，个人可以依法向法院提起诉讼。

从实践来看，围绕着个人信息权益的行使与救济问题产生了不少争议，如个人是否必须先向处理者主张权利，甚至先向履行个人信息保护职责的部门投诉无果后，才能起诉等。建议司法解释对**行使查阅、复制其个人信息的范围、更正补充权的行使以及错误更正补充的赔偿责任、删除权的司法救济以及民事责任**等内容进行规定。

建议三：明确侵权的归责原则、构成要件与赔偿责任

个人信息侵权责任涉及到《民法典》与《个保法》的关系，以及个人信息权益与隐私权、肖像权等其他人格权益的适用，还包括对于个人信息侵权责任的构成要件的理解与适用问题。因此，建议司法解释至少应当对**侵害隐私权与个人信息权益的归责原则的适用关系、侵害隐私权与个人信息权益的归责原则的适用关系、侵害隐私权与个人信息权益的归责原则的适用关系**等问题进行明确。

https://mp.weixin.qq.com/s/G17lj0-tE8V5ML-6lOec9A

3、在变化中寻找解法 数据安全为数字经济发展保驾护航

在全球发展不断变化的今天,我们要建立起与数字经济相适应的生产关系,最重要的是数据确权问题。中国友谊促进会理事长、公安部原副部长、国家网信办原副主任陈智敏认为,可以从五个维度来考虑数据确权问题:

一是坚持主体在民,数据的主体是人民群众。

二是主权在国,数据的管理权、控制权、发展权、司法组织权、国与国之间的网络反制权,都应该由国家掌握。

三是企业开发。要保护企业的数据使用权、开发权,赋予企业数据交易权。

四是对数据要共享共用。数据创造出来的利益,应该在国家以税收、企业以利润、公民以收入来共享。同时,数据要共用,国家掌握的公共数据要开放,企业的数据要有偿相互开放,公民的数据也应该按照相关的法律法规对社会开放。

五是数据要跨境流动、合作共赢。要依据相应的法律,给相关的部门、企业、公民数据跨境流动的权利。

“数据跨境流动是一个客观的规律,我们要充分认识到这个基本特征。在这个认识基础上,数据跨境流动一定要坚持公平公正、互利、合作共赢的原则。”陈智敏表示,在联合国的框

架内,我们可以运用平等、公正、相互尊重、互利的原则,逐步建立数字经济的发展规则,从双边多边区域性的数字发展开始,逐步扩散到全球,进而推动全球数字经济的跨境发展与管理。

vivo 首席安全官鲁京辉认为,公司在运营跨境业务时,保护数据安全也至关重要。首先,在全球业务拓展的时候,企业应严格遵守所在国家和地区的监管要求。其次,企业要勇于承担维护数据安全的责任,充分将安全和隐私保护的特性嵌入产品服务中。同时,企业也要不断提供新的技术创新,通过创新给消费者提供一个更安全的环境。

http://www.ciia.org.cn/news/20769.cshtml

4、数据安全亟需细化管理要求 专家:应从生产安全角度发力治理

3 月 28 日,由中国网络安全产业联盟主办的 2023 年 CCIA 网络安全技术应用专题研讨会在北京召开。全知科技 CEO 方兴从技术的角度切入,分享了数据安全行业的建设思考。他指出,原来讲的数据安全是高价值信息在数据载体上的安全,随着大数据、AI 技术的发展,不需靠人推导,靠机器就可以从数据当中挖掘知识和情报。**对数据的保护也应该从一个资产层的角度向生产层转变,由已获高价值信息的防**

御性保护转向全流程保护，特别当今数据已成为生产要素，加速流通的背景下。

“针对生产要素去进行保护，实际上比资产层面保护要困难得多。这是我理解为什么现在要把数据安全单独拿出来跟原来的网络安全并列，因为它产生了完全不同的视角。”方兴说道，这种数据既有价值，但是对它处理不善可能带来危害，变成了生产安全的视角，这是我理解的数据安全为什么在这个时代这么重要。

生产者要考虑生产过程效率的平衡，要关注全流程，而数据却如此庞大和繁杂，在流通环节，落地《数据安全法》和数据安全成了极具挑战的事情。

“在这个当中，从数据的资产认定到数据在什么地方暴露，要形成数据暴露面的概念，数据暴露面在整个数据处理活动又会产生什么样的数据活动，数据又能流向到哪里，数据采集了之后用到什么场景等等。如果这些东西都刻画不清楚，我认为一个企业它是做不好数据安全的。”

方兴表示，这需要重新构建一个数据流动的体系模型，解决“看清”数据的问题，搞清楚到底有哪些资产，这些资产到底在怎样流通，到底去了哪里。

方兴进一步指出，**监管需要细化数据安全的管理要求，指导各行各业制定相应的重要数据目录。有了明确的管理细**

则，企业才能更好地去执行和落地；拥有数据清晰或范围明确的目录，则有利于数据安全工作的开展。

他建议，**国家应牵头成立数据风险监测和预警体系，包括对积极发现风险、处置风险的单位给予更多正向的激励，**而不是反向的打击。各界通过协同构建数据安全合作生态，及时发现风险，并快速响应、处理风险，守护数据安全。

https://www.21jingji.com/article/20230329/herald/04402cd971ab861a0069c5880cb1f0ee.html

5、AIGC 领域风险事件频发 亟须立法保障产业可持续发展

3 月 31 日，光明网报道，一位女网友在网上晒出自己在地铁列车的照片被别有用心的网友下载，并用 AIGC 技术“一键脱衣”，造谣图随后在网上广泛传播。此事引发网友关注并冲上热搜，不少网友怒斥：“科技不应该用在这上面！”

2021 年，我国发布的《法治中国建设规划（2020-2025 年）》当中明确提出，加强信息技术领域立法，及时跟进研究数字经济、互联网金融、人工智能、大数据、云计算等相关法律制度，抓紧补齐短板。加强区域协调发展法律制度建设。制定和修改法律法规要着力解决违法成本过低、处罚力度不足问题。

长年深耕人工智能领域的湖南大学信息科学与工程学

院博士生导师、教授张大方多次**呼吁对 AIGC 领域尽早立法**。

张大方向《证券日报》记者阐述了对 AIGC 领域立法工作的“四条红线”思路，“**AIGC 立法当中应有‘四条红线’思路，即 AIGC 技术不能危害全人类共同的生存、和平、发展的利益**，不能颠覆国际国内社会所公认的公平正义，不能侵害个人的合法权益，不能妨害相关产业的正常健康发展。在 AIGC 的理念提出、框架设立、工作原理、模型开发、数据收集、用户交互、使用场景等领域都应有法律覆盖，应当既有对 AIGC 产业发展的整体法，也有对 AIGC 开发、使用、传播、审定等环节的专门法，还应当与国际法规条例进行接轨，便于日后实施国际司法协助。”

https://finance.sina.com.cn/jjxw/2023-04-03/doc-imynzmez0386549.shtml

数据安全事件

1、纽约律师事务所因未能保护健康数据而被罚款 20 万美元

3 月 29 日，据外媒报道，一家纽约律师事务所（HPMB）已同意向该州支付 200,000 美元的罚款，因为它未能保护大约 114,000 名患者的私人和电子健康信息。HPMB 与纽约市地区许多医院有业务关系往来，帮助维护患者的敏感私人信息。

2021 年 11 月，攻击者利用 HPMB 的混合 Exchange 管理服务器中的一个漏洞访问了该公司的系统。去年 12 月，攻击者在 HPMB 的系统上部署了 Lockbit 勒索软件变体。而 Microsoft 已在几个月前发布了针对此漏洞的补丁，但 HPMB 并未及时应用这些补丁。

HPMB 的数据安全故障不仅违反了州法律，还违反了 HIPAA。该公司未能采取 HIPAA 要求的几项措施，包括对其系统进行定期风险评估、加密其服务器上的私人信息以及采取适当的数据最小必要原则。

https://www.helpnetsecurity.com/2023/03/29/new-york-law-firm-fined-200k-failing-protect-health-data/

2、澳大利亚赌场皇冠度假集团披露遭受 Clop 勒索软件攻击后，发生数据泄露

3 月 29 日，据外媒报道，澳大利亚博彩和娱乐巨头皇冠度假村披露了一起由利用最近发现的 GoAnywhere 零日漏洞引起的数据泄露事件。

“他们声称他们非法获取了数量有限的官方文件，但我们可以确认没有客户数据遭到泄露。”该公司表示道。

Clop 勒索软件组织声称通过利用 Fortra 的 GoAnywhere MFT 安全文件传输工具中的零日漏洞（CVE-2023-0669）从 130 多个组织窃取了敏感数据。

https://securityaffairs.com/144193/data-breach/crown-resorts-clop-ransomware.html

3、印度著名制药公司 Sun Pharmaceutical 遭受网络攻击确认，ALPHV 声称对此事负责

3 月 28 日，据外媒报道，印度最著名的制药公司之一 Sun Pharmaceutical Industries Ltd. 遭遇了重大数据泄露事件。该公司证实，其 IT 系统在网络攻击中受到影响，ALPHV 勒索软件组织声称对此次攻击负责，并表示他们已经从该公司访问了超过 17TB 的数据。这包括有关客户和供应商的敏感信息以及有关 1,500 多名美国员工的完整文件。

https://thecyberexpress.com/sun-pharma-cyber-attack/

4、加州法院要求 GitHub 提供 Twitter 源代码泄密者信息

Cybernews 网站消息，Twitter 向美国北加州地区法院提出申请，希望代码托管平台 GitHub 能够提供源代码泄露者的具体信息。目前，法院已经批准，并要求 GitHub 在 4 月 3 号之前，提供发布者详细的身份信息，包括“所有识别信息，涵盖姓名、地址、电话号码、电子邮件地址、社交媒体资料数据和 IP 地址”。

https://cybernews.com/news/court-forces-github-reveal-twitter-source-code-leaker/

5、宝马潜在的数据泄露使客户信息面临风险

3 月 29 日消息，Play 勒索软件组织声称对 BMW France 的网络攻击负责。如果在 2023 年 4 月 9 日之前不满足赎金要求，这个臭名昭著的组织威胁要在暗网上发布被盗数据。该组织声称可以访问宝马客户的文件、合同、财务信息等。

与其他勒索软件团体一样，Play 使用各种策略来访问组织的系统，例如网络钓鱼电子邮件、利用漏洞和破坏远程桌面协议。一旦他们获得访问权限，他们就会加密受害者的文件并要求为解密密钥支付赎金。虽然该安全事件尚未得到宝

马法国公司的证实，但潜在网络攻击的消息再次将数据泄露问题推上了风口浪尖。

https://thecyberexpress.com/bmw-data-breach-customers-information-risk/

6、400 万患者信息泄露，公司：提供免费信用检测作为赔偿

3 月 30 日报道，Independent Living Systems (LLS) 是一家面向老年人、残障人士和受损人士的医疗保健设施提供商，这家医疗保健提供商最近遭受了大规模的网络攻击。这次攻击对公司的文件系统造成了重大破坏，并泄露了多达 400 万人的个人数据，包括社会安全号码和其他受保护的信息，这些人可能会面临遭受财务或信用损失的风险。

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

7、Latitude Financial 泄露了数百万用户的个人数据

3 月 27 日报道，澳大利亚非银行贷款机构 Latitude Financial 透露，本月早些时候对其系统的网络攻击比最初想象的影响更为广泛。

该公司于 3 月 16 日首次宣布该漏洞，称约 330,000 人的数据已被泄露。然而，在近日澳大利亚证券交易所的更新中，Latitude 承认可能有多达 800 万人的个人信息被盗。

据称，黑客已经获取了客户的姓名、地址、出生日期、电话号码、护照号码，在某些情况下还获取了月度财务报表。该公司仍在评估重复记录的数量，并确定受影响客户的真实数量。

https://www.cyberkendra.com/2023/03/latitude-financial-cyber-hack-exposes.html

8、黑客入侵英国养老金保护基金，窃取员工数据

3 月 28 日报道，黑客利用第三方数据传输服务，窃取了一家英国养老金保护基金部分员工的数据。

该基金发言人珍妮·彼得斯(Jenny Peters)在一份声明中表示，“黑客通过 GoAnywhere 访问了该基金的一些数据，该基金使用 GoAnywhere 进行一些安全数据传输。但被盗信息与我们的会员或退休人员无关。”勒索软件团伙 Clop 周四声称攻击了该组织，并且在其网站上发布了一篇文章，将该养老金保护基金列为最近的受害者之一。

https://cn.dailyeconomic.com/tech/2023/03/28/26299.html

9、泄露用户信息长达一年半，丰田被服务商坑惨了

全球知名汽车制造公司丰田（TOYOTA）遭遇了严重的用户信息泄露事件。安全研究人员发现，黑客通过攻击丰田

意大利数字营销自动化和分析软件服务提供商 Salesforce Marketing Cloud，从而获得了海量的用户数据，且至今为止数据泄露已有一年半之久。

此外，丰田意大利还泄露了软件公司 Mapbox 的应用程序编程接口 (API) 令牌，导致敏感数据泄露范围增大。攻击者可能会借此获取丰田意大利用户的手机号码和电子邮箱等，并利用这些信息发起网络钓鱼攻击。

好消息是，截止到发稿时，丰田意大利已经将这些数据再次保护起来，该公司也表示，已经和第三方网络安全公司合作，采取了额外的措施加强其网络安全系统和协议。

https://www.freebuf.com/news/361832.html

10、宝洁公司确认 GoAnywhere 漏洞泄露

3 月 28 日报道，美国消费品巨头宝洁公司 (P&G) 证实其旗下一家公司受到了 Fortra 的 GoAnywhere 漏洞的影响。

宝洁在声明中表示，攻击者获得了有关该公司员工的部分信息，“但未经授权方获得的数据不包括社会安全号码或国民身份证号码、信用卡详细信息或银行账户信息等信息。”宝洁公司声称，该公司在 2 月初得知了这起事件，随后立即展开调查，禁止使用 Fortra 的服务，并通知公司员工有关本次网络攻击的信息。

https://cybernews.com/news/procter-gamble-goanywhere-bug-breach-clop/

11、TMX Finance 及其子公司约 480 万个客户的数据泄露

媒体 3 月 31 日称，TMX Finance 及其子公司 TitleMax、TitleBucks 和 InstaLoan 披露了一起数据泄露事件，涉及 4822580 个客户的数据。这家加拿大金融公司表示，黑客在 2022 年 12 月上旬入侵了其系统，但他们直到 2023 年 2 月 13 日才发现了攻击活动。3 月 1 日完成内部调查后，TMX 发现攻击者在 2023 年 2 月 3 日至 14 日窃取了客户的信息，包括姓名、护照号、驾照号码、税号、社会安全号码和金融账户信息等。现在，该公司实施了端点保护和监控，重置了所有员工帐户密码，并将为用户提供 Experian 为期 12 个月的身份保护服务。

https://www.bleepingcomputer.com/news/security/consumer-lender-tmx-discloses-data-breach-impacting-48-million-people/

12、美国购债公司 NCB 遭到攻击近 50 万客户的财务信息泄露

3 月 29 日，据媒体报道，美国购债公司 NCB Management Services 遭到攻击，近 50 万客户的财务信息泄露。NCB 于 2

月 4 日发现，未经授权的第三方于 2 月 1 日获得了 NCB 系统的访问权限，并于 3 月 8 日确认客户与美国银行信用卡账户相关的一些信息泄露。该事件涉及 494969 人的姓名、驾照号码、社会安全号码、信用卡号码、路由号码、账户余额和账户状态等。美国银行将为受影响的个人提供 Experian IdentityWorksSM 两年的身份盗窃保护服务。

https://therecord.media/debt-buyer-cyberattack-data-breach

《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