全球数据安全观察

总第 119 期 2022 年第 47 期

(2022.12.19-2022.12.25)

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
1、《关于构建数据基础制度更好发挥数据要素作用的意见》发布.....1
2、《非法证券活动网上信息内容治理工作方案》印发.....1
3、美国总统拜登正式签署《量子计算网络安全防范法》...2
技术、产品与市场.....3
1、行业：ISC 数字安全创新能力全景图谱发布，打造首个数字安全维基百科.....3
2、2023 中国数据安全发展趋势十大预测.....4
3、Zscaler：85%的攻击使用加密通道.....5
4、研究：2022 年美国受金融业数据泄露影响最大.....6
5、2023 年值得关注的 5 大云安全威胁.....7
业界观点.....9
1、工信部网安局：四方面发力抓好数据安全工作.....9
2、吴沈括：构筑面向数字化和全球化的数据跨境流通生态.....10
3、完善数据要素治理制度，保障数据流通交易安全.....12
4、姚期智、郁昱：奋力攻坚关键核心技术 加快构建数据基础制度.....13
5、筑牢数字安全屏障，完善企业数据安全治理.....15

数据安全事件 17
1、Meta 以 7.25 亿美元和解隐私集体诉讼 17
2、微软未经用户同意使用广告插件，被罚 6000 万欧元 ... 17
3、伊利诺伊州生育中心数据泄露 45 万美元的集体诉讼和解 18
4、莫利公司数据泄露 430 万美元的集体诉讼和解 18
5、Epic Games 因违反隐私法等原因被 FTC 罚款 5.2 亿美元 19
6、黑客出售据称是从 Gemini 窃取的 570 万用户的信息 ... 20
7、IAM 巨头 Okta 源代码泄露 20
8、黑客出售 4 亿 Twitter 用户数据库 21
9、蔚来遭遇数据泄露，被勒索 225 万美元等额比特币 22
10、鞋类品牌 Ecco 在 500 天内泄露超 60GB 敏感数据 23
11、体育博彩公司 BetMGM 披露数据泄露事件 23
12、俄罗斯黑客组织 Killnet 声称：已窃取 FBI 上万特工的个人数据 24
13、LastPass 承认严重数据泄露，加密密码库被盗 25
14、德国连锁酒店 H-Hotels 遭 Play 勒索软件攻击，客户数据疑泄露 25
15、McGraw Hill 的 AWS S3 存储桶配置错误泄露 22TB 数据 26

政策形势

1、《关于构建数据基础制度更好发挥数据要素作用的意见》发布

12 月 19 日，中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》。对强化数据安全保障体系建设、加强数据分类分级管理作出强调，并明确要求构建数据安全合规有序跨境流通机制。

http://www.gov.cn/xinwen/2022-12/19/content_5732695.htm

2、《非法证券活动网上信息内容治理工作方案》印发

为切实维护人民群众财产安全，进一步规范证券活动网上信息内容，严厉打击股市“黑嘴”、非法荐股等行为，打造清朗网络空间，12 月 23 日，中央网信办秘书局、中国证监会办公厅关于印发《非法证券活动网上信息内容治理工作方案》，提出以下举措：清理处置涉非法证券活动的信息、账号和网站；清理处置涉非法证券活动的信息、账号和网站；建立健全非法证券活动网上信息内容常态化处置工作机制；加强网上宣传引导助力投资者提高风险防范意识。

http://www.cac.gov.cn/2022-12/23/c_1673432294970963.htm

3、美国总统拜登正式签署《量子计算网络安全防范法》

12 月 21 日，美国总统拜登正式签署《量子计算网络安全防范法》（Quantum Computing Cybersecurity Preparedness Act），旨在应对信息技术系统向后量子密码（PQC）迁移的风险。该法强调“PQC 迁移和评估”，规定在国家标准与技术研究院（NIST）院长发布 PQC 标准后 1 年内，管理和预算办公室（OMB）主任应当发布指导意见，要求各机构优先考虑 OMB 提出的重点信息技术，并根据此优先顺序制定本机构信息技术向 PQC 迁移的计划。

https://www.secrss.com/articles/50353

技术、产品与市场

1、行业：ISC 数字安全创新能力全景图谱发布，打造首个数字安全维基百科

近日，ISC 2022 数字安全创新能力百强（以下简称“创新百强”）正式发布 ISC 2022 数字安全创新能力全景图谱。

经过对整体数字安全行业的创新领域重新进行了一轮深度梳理，最终为凝结为 ISC 2022 数字安全创新能力全景图谱中数据安全、安全运营、供应链与应用安全、工业互联网安全、威胁检测与响应、攻击面与资产管理、云安全、零信任、安全访问服务边缘 SASE、流量安全、移动安全、身份安全、密码管理的 14 个领域维度，全面覆盖了数字安全当下的热点技术方向，将有效助力洞见行业未来的发展趋势。

本次发布的 ISC 2022 数字安全创新能力全景图谱全面收录了参选 ISC 创新百强的 300 余家数字安全创新厂商。同时，它也是一套动态的评估体系，未来其将对具有创新性的数字安全产品、解决方案、应用案例等进行多维度展示，并及时对数字安全领域以及所属厂商进行追踪，按周期完成对各类数据的更新。

https://mp.weixin.qq.com/s/Vb13WsmfVPV-ko4dP2L0RQ

2、2023 中国数据安全发展趋势十大预测

在即将到来的 2023 年，数据安全形势将愈加复杂。日前，明朝万达公司数据安全专家对数据安全领域未来一年发展的趋势进行了预测，以更好地帮助企业在应对新的数据相关问题时做好准备。

趋势 1：数据安全政策法规日益完善下亟需配套的监管检查产品技术支撑

趋势 2：组织的安全体系建设由满足被动合规需要逐步转向业务融合的实战化落地

趋势 3：数据安全治理成为数据安全体系建设的桥头堡，并为体系化防护垫定基础

趋势 4：组织的数据安全风险需要依赖系统化、产品化技术手段构建全生命周期管控

趋势 5：个人信息及隐私保护成为组织数据安全体系建设的主战场

趋势 6：如何安全地最大化挖掘释放政务数据价值成为各大数据局等主管部门的重点方向

趋势 7：跨组织、跨区域之间数据安全共享推动隐私计算等技术广泛应用

趋势 8：数据出境安全逐渐从满足监管自评估备案到自建设安全防护阶段转变

趋势 9：数据主权维护面临的挑战愈加严峻，且需警惕“新数字孤立主义”倾向

趋势 10：数字版权相关技术方案和管理体系发展步入正轨

https://mp.weixin.qq.com/s/1KbWleTHssBMAST0SecdVw

3、Zscaler：85%的攻击使用加密通道

根据 Zscaler 的最新报告，加密攻击仍然是世界各国网络安全专家面临的一个重大威胁。美国、印度和日本在过去 12 个月中遭受的加密攻击增幅最大。

加密攻击国家 TOP5： 2022 年被加密攻击最多针对的

五个国家分别是美国、印度、南非、英国和澳大利亚。其中南非是今年 TOP5 的新面孔，将法国挤出了 TOP5，日本（613%）、美国（155%）和印度（87%）的加密攻击都同比大幅上升。

制造业和教育行业风险最大：加密攻击并非无差别地攻击所有行业，部署传统安全解决方案的企业往往比其他行业更容易成为受害者。今年，制造业遭受的加密攻击增加了 239%，取代科技行业成为 2022 年被加密攻击最多的行业。加密攻击增幅第二大的行业是教育，同比增长 132%。此前，从 2020 年到 2021 年，教育行业的加密攻击增加了 50%。教育和制造业等行业从零信任架构中受益最多，该架构能够检查所有互联网绑定流量，以识别可疑活动并降低加密攻击日益增长的风险。

https://www.secrss.com/articles/50228

4、研究：2022 年美国受金融业数据泄露影响最大

根据 Flashpoint 于 2022 年 12 月 20 日发布的报告显示，金融行业在 2022 年的数据泄露事件中位居所有行业的第二位。美国是受影响最严重的国家，其次是阿根廷、巴西和中国。

这些针对全球金融机构的违规行为中，约有 57% 归因

于“一般黑客攻击”。相比之下，大约 6.5% 是 ATM 窃取的结果，这是一种通过操纵带有隐藏记录设备的机器来针对信用卡和借记卡的 PIN 窃取技术。

Flashpoint 还发现了一些在 2022 年以金融机构为目标的勒索软件组织，包括 LockBit、Conti 和 Corp Leaks。

https://www.infosecurity-magazine.com/news/us-most-impacted-data-breaches/?&web_view=true

5、2023 年值得关注的 5 大云安全威胁

orca.security 对 2023 年云安全发展趋势进行了研究和预测，并总结了企业组织应该重点关注的 5 大云安全威胁。

（1）云上暴力攻击

调查数据显示，与 2021 年相比，2022 年针对企业组织的网络暴力攻击数量增加了 31%。值得一提的是，其峰值与重大地缘政治和社会经济事件存在很大关联。因此，攻击者试图用暴力手段或其他可用的漏洞入侵企业云上资产只是时间问题，并且很快就会到来。

（2）API 威胁

据《2022 年公共云安全状况报告》数据显示，高达 70% 的企业组织中，存在可公开访问的 API 服务器，这使得 API 应用服务面临着巨大的网络攻击安全隐患。

包括 Gartner 在内的安全研究公司一直警告称，API 服务器攻击预计将在未来几年持续增长，而且在 2022 年也已显露苗头。有鉴于此，研究人员预计保护云上 API 应用安全将在 2023 年成为企业组织和安全运营团队的重要任务。

（3）错误的云配置和影子数据

在云中，数据被大量存储在数据库、存储桶或 Blob 容器中，随着云上存储的数据不断增长，数据攻击面每年也都在快速增加。2022 年里，我们目睹了很多严重的云上数据安全事件，其中很多都是由错误的云配置所引起的。

（4）CI/CD 和供应链攻击

对于黑客而言，CI/CD（持续集成和持续交付）环境是极具吸引力的攻击目标，从 npm 服务仓库和 python 代码，到管道执行（PPE），所有这些都是攻击者们可能发起攻击的新途径。在 2022 年，一些部署了这些攻击战术的恶意软件已经展示了供应链攻击实现的容易程度。

（5）安全漏洞

据美国国家漏洞库（NVD）数据所示，自 2017 年以来，已知的 CVE 数量正在不断增加。在即将到来的 2023 年，我们将继续看到越来越多的安全漏洞，这意味着组织将面临更多的修补工作。因此，优先级排序和了解应该首先修补哪个漏洞将变得更加重要。

https://www.secrss.com/articles/50196

业界观点

1、工信部网安局：四方面发力抓好数据安全工作

近日，在 2022 中国互联网大会数据安全论坛上，工业和信息化部网络安全管理局副局长杜广达讲道，当前，电信和互联网领域占全国行业机构产生数据总量超过四分之一，做好电信和互联网领域数据安全工作，就是守住行业标准底线与国家数据安全的核心所在。

“当前电信和互联网行业数据安全工作仍处在构建完善的起步阶段，相关制度机制、标准规范和技术能力尚在梯次导入过程中。”杜广达讲道。

他指出，践行总体国家安全观，统筹发展和安全，立足行业数据安全工作新定位和新要求，重点要抓好以下四个方面的工作。

（1）以重要数据识别备案为核心，夯实安全工作基础。重要数据保护是行业数据安全管理工作的重心和根本目标。

（2）以数据安全风险防范为重点，探索开展安全实践.准确把握数据安全风险发生的规律、动向和趋势，有效防范和处置数据安全风险，是维护数据安全的发力点。

（3）以数据安全技术手段为抓手，强化以技管术能力。长期实践证明，强有力的技术手段是企业落实主体责任和监管部门履职尽责的核心战略。

（4）以数据安全产业生态为支撑，提升安全保障水平。保障数据安全离不开数据安全技术和产品的有力支撑。

https://www.wangan.com/p/11v6be3bb03a781a

2、吴沈括：构筑面向数字化和全球化的数据跨境流通生态

近日，《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》出台，全面检视域外有关数据跨境流动治理的理念举措及其成败得失，着力从四个方面系统地勾勒了一幅多方主体有序共建、共治、共享的多维生态图景：

一是**国际合作生态**。一方面，《意见》务实回应产业现实需要，重点突出地要求开展数据交互、业务互通、监管互认、服务共享等方面的国际交流合作，进而推动各项发展瓶颈的及时突破；另一方面，《意见》敏锐研判国际前沿趋势，方向明晰地要求以《全球数据安全倡议》为基础，积极参与数据流动、数据安全、认证评估、数字货币等国际规则和数字技术标准制定，进而提升我国在全球数据流通生态中的战略地位。

二是**开放市场生态**。《意见》强调坚持开放发展，推动数

据跨境双向有序流通，鼓励国内外企业及组织依法开展数据跨境流动业务合作，支持外资依法依规进入开放领域，推动形成公平竞争的国际化市场。着眼国内国际双循环相互促进的新发展格局，妥善平衡和融合国内外各方市场主体的需求与期待，充分激励和调动其有序参与的积极性，从而更好地利用国际国内两个数据市场、两种数据资源。

三是**数据治理生态**。《意见》以数据治理领域的现行政策战略和法律法规为依据，要求统筹数据开发利用和数据安全保护，探索建立跨境数据分类分级管理机制。特别是在《网络安全法》《数据安全法》《个人信息保护法》等新一代数据立法框架下，数据分类分级是国家数据安全保护的基础性制度，而现代数据治理的核心方法论便体现为，以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

四是**协作监管生态**。《意见》直面新技术环境下数据跨境流动的特殊场景属性和监管执法特点，精准分析总结国内外监管机制及其变革规律，强调探索构建多渠道、便利化的数据跨境流动监管机制，健全多部门协调配合的数据跨境流动监管体系。同时，《意见》也强调，对影响或者可能影响国家安全的数据处理、数据跨境传输、外资并购等活动依法依规进行国家安全审查，并且应当按照对等原则对维护国家安全

和利益、履行国际义务相关的属于管制物项的数据依法依规实施出口管制，保障数据用于合法用途，防范数据出境安全风险。毋庸置疑，在当下高度自动化、智能化的数据跨境实务场景中，敏捷、高效的监管机制是保障数据流动畅通和业务运行延续的基础条件，而立体、协同的监管体系更是确保数据流转利用全生命周期安全的关键一环。

https://mp.weixin.qq.com/s/VDdd9Uanr2NKv2WpMnmFIw

3、完善数据要素治理制度，保障数据流通交易安全

近日，中共中央 国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》（简称《数据二十条》），结合当前数据要素市场发展总体趋势和要求，从安全与发展、法治与行业自治、政府监管与市场自律等方面出发，明确了数据要素安全治理的制度规则、管理标准与创新机制。

（一）“保安全”：数据安全是数据要素流通交易的底线；

（二）“重发展”：发挥政府有序引导和规范发展的作用；

（三）“促创新”：对于探索性创新的领域建立容错机制。

《数据二十条》从构建新发展格局、推动高质量发展的战略高度，统筹考虑政府、企业和社会三方职责，重点下好数据流通交易三步“先手棋”。

（一）建立监管机制，创新政府数据治理思路；

（二）压实企业责任，推动企业积极参与治理；

（三）强化多元协同，发挥社会力量协同治理。

数据要素基础制度立足我国数字经济发展现状，针对数据流通交易中的确权难、监管难等问题，构筑起防范数据流通交易风险的三道“安全线”。

（一）完善制度设计；

（二）鼓励多方协同；

（三）强化技术创新。

https://www.secrss.com/articles/50235

4、姚期智、郁昱：奋力攻坚关键核心技术 加快构建数据基础制度

数字经济的核心要素包含数据、模型算法、算力等方面。数据正在成为经济关键生产要素，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。我们需要研究推进数据确权和分类分级管理，畅通数据交易流动，完善数据合理定价，实现数据要素市场化配置，合理分配数据要素收益。

利用创新技术手段加快培育数据要素市场。在符合个人信息保护法、数据安全法等相关法律法规要求的前提下，利

用安全多方计算技术打破“数据孤岛”，实现数据要素在数据安全和隐私保护基础上有序流通。探索开展数据质量标准化体系建设，加快推进数据采集和流通交易接口的标准化，促进数据整合互通和互操作。围绕数字化转型，打造“数据中台”，在数据安全、数据隐私合规的前提下进行全面整合；同时，建设企业间的合作联盟，打造行业级的隐私计算平台，形成企业间的数据要素流通市场。

算法模型治理是人工智能的下一篇章。算法模型的治理，即模型的可解释性、模型的精度与风险、算法公平性等方面。模型治理既是技术，又是制度，成熟的数字化企业会形成完整的模型治理制度。在推广建设人工智能能力的同时，也要推广成熟的模型治理制度建设。目前，包括对抗攻击、因果分析与可解释性分析的研究工作已经给这方面的工作指出了发展方向。在这些方面，我们认为应该进行以下工作内容：**一是建立模型治理制度，形成模型价值评估、精度评估、风险与缺陷管理的成熟体系。二是建立模型评测中心，结合各类场景牵头建设数据模型标准，并实践模型评测，赋能行业发展**。

建设数字经济离不开算力的支持。算力在数字经济建设过程中的必要性，主要体现在五方面：一是数据模型需要在算力平台上实现；二是在海量数据、海量模型、实时计算的

数字化时代，对算力的要求急剧提升；三是建立数据要素流通市场，多方数据共同建模使得对算力的要求更高；四是创新型软硬件体系架构、智能芯片以及未来的量子计算技术对算力都有较大需求；五是从数据要素安全的角度来讲，算法是攻防双方的主要角力点，更高的算力支持，能够有效增加不法分子窃取数据的成本，从而降低安全风险。

https://mp.weixin.qq.com/s/IwFewFIaIRrOsRl4twgs8w

5、筑牢数字安全屏障，完善企业数据安全治理

近年来，我国在筑牢数字安全屏障方面做了不少工作，取得一定成绩，出台了国家安全法、密码法、数据安全法、个人信息保护法等一系列法律法规，构筑起维护数据安全和促进数字经济持续健康发展的法律制度保障。也要看到，我国在完善企业数据安全治理、保障企业数据安全方面还存在一些短板弱项，比如**数据安全治理主体责任不明晰，企业数据安全治理流程及效果评价尚未形成统一标准，部分企业对数据安全不够重视，黑客攻击造成企业数据泄露**等。单纯依靠企业自身的力量难以解决这些问题，必须加快探索构建由政府部门、企业、社会组织、网民等共同参与的企业数据安全协同治理体系，共同保障企业数据安全，织密织牢国家数据安全网。

加快构建政府、企业、社会多方协同治理模式，强化分行业监管和跨行业协同监管，压实企业数据安全责任，努力实现更优的数据安全治理效果，是完善企业数据安全治理、维护企业数据安全的重要内容。一方面，积极发挥政府和行业协会等主体作用，加强对数据安全治理规则、相关标准制定的组织引导，强化对企业数据安全的监督监管，确保关键领域和核心环节的数据安全。另一方面，进一步明确各类平台和企业等市场主体在数据安全治理方面的责任，提高居民个体维护自身数据安全的意识和积极性，同心协力维护数据安全，夯实数字经济持续健康发展的安全基础。

https://www.wangan.com/p/11v6c8f924fb864d

数据安全事件

1、Meta 以 7.25 亿美元和解隐私集体诉讼

12 月 23 日报道，因 2018 年 3 月爆出的数据挖掘公司 Cambridge Analytica 未经同意收集数千万 Facebook 用户信息的丑闻，Meta/Facebook 遭遇了集体诉讼，本周五双方宣布达成了和解协议，和解金额高达 7.25 亿美元，为美国至今金额最高的与隐私相关的集体诉讼和解案。Cambridge Analytica 已在 2018 年 5 月停止运营。

https://www.solidot.org/story?sid=73744

2、微软未经用户同意使用广告插件，被罚 6000 万欧元

12 月 25 日，据外媒报道，法国隐私监管机构对微软爱尔兰子公司处以 6000 万欧元罚款，原因是其在未经客户明确同意的情况下使用广告 cookie。这种做法违反了欧洲数据保护法。

经调查，微软没有为 Bing 搜索引擎的主页实施“拒绝 cookie 与接受 cookie 一样容易的机制”。据华尔街日报称，目前微软已经通过实施拒绝广告 cookie 的选项解决了这个问题。

https://securityaffairs.co/wordpress/139982/breaking-

news/microsoft-fined-e60m.html

3、伊利诺伊州生育中心数据泄露 45 万美元的集体诉讼和解

12 月 20 日，据外媒报道，伊利诺伊州生育中心 (FCI) 同意支付 450,000 美元，以结束声称其通过不合格的网络安全措施造成 2021 年数据泄露的说法。

据称，在泄露期间，第三方获得了其客户的社会安全号码、护照号码、支付卡信息、医疗保健数据、保险信息和近 80,000 名患者的其他标识符。据报道，该违规行为还泄露了其他员工信息。

受影响的消费者对 FCI 提起集体诉讼，认为该公司本应通过合理的网络安全措施保护他们的个人信息。FCI 尚未承认有任何不当行为，但同意以 450,000 美元的集体诉讼和解金来解决这些指控。

https://topclassactions.com/lawsuit-settlements/privacy/data-breach/fertility-centers-of-illinois-data-breach-450k-class-action-settlement/?web_view=true

4、莫利公司数据泄露 430 万美元的集体诉讼和解

12 月 21 日，据外媒报道，莫利公司（Morley Companies

Inc.）已拨出 430 万美元来解决集体诉讼，原因是在 21 年 8 月其遭受的勒索软件攻击事件中，莫利的客户数据遭到泄露。

Morley Companies 是一家位于密歇根州的公司，提供业务流程外包（例如客户服务台、销售和营销支持）、会议、奖励展览和展示等服务。Morley 已将数据泄露事件通知了超过 694,000 人，泄露期间暴露的信息包括客户的社会安全号码、姓名、地址、出生日期、驾照号码以及医疗和健康信息。

莫利公司否认有不当行为，但已同意诉讼和解，以减轻正在进行的诉讼的风险和成本。

https://topclassactions.com/lawsuit-settlements/privacy/data-breach/morley-companies-data-breach-4-3m-class-action-settlement/?web_view=true

5、Epic Games 因违反隐私法等原因被 FTC 罚款 5.2 亿美元

据 12 月 19 日报道，堡垒之夜的制造商 Epic Games 将支付 5.2 亿美元，以和解有关违反儿童隐私法和使用黑暗模式诱使数百万游戏玩家进行无意消费的指控。FTC 在投诉中称，Epic 在未通知或未征得其父母同意的情况下，收集 13 岁以下玩家的信息违反了 COPPA，被罚款 2.75 亿美元。此外，它还使用黑暗模式欺骗包括儿童和青少年在内的 Fortnite 玩家进行不需要的游戏内购买，须向受影响客户支付 2.45 亿美

元的退款。目前，该公司已改进默认隐私设置，并更改了支付流程以防不必要的收费。

https://www.bleepingcomputer.com/news/gaming/epic-games-to-pay-520-million-for-privacy-violations-dark-patterns/

6、黑客出售据称是从 Gemini 窃取的 570 万用户的信息

媒体 12 月 15 日称，黑客在多个暗网平台出售据称是来自 Gemini 的数据库，包含 570 万用户的信息。加密货币交易所 Gemini 近期发布通知称，第三方供应商遭到了网络攻击，未经授权的攻击者窃取了 Gemini 客户的邮件地址和电话号码，目前已有客户收到了钓鱼电子邮件。该数据库似乎在 9 月起就开始出售，当是价格为 30 个比特币（约合 520000 美元）。Gemini 建议客户使用强大的身份验证方法，并建议激活 2FA 保护或使用硬件安全密钥来访问帐户。

https://securityaffairs.co/wordpress/139742/data-breach/5-7m-gemini-users-leak.html

7、IAM 巨头 Okta 源代码泄露

12 月 22 日消息，著名身份验证和 IAM 解决方案提供商 Okta 披露其私有 GitHub 存储库本月遭到黑客攻击，源代码遭泄露。

本月早些时候，GitHub 曾提醒 Okta 其代码存储库遭可疑访问。“经调查，我们得出结论，这种非法访问被用来复制 Okta 代码存储库。”该公司首席安全官（CSO）David Bradbury 在电子邮件中写道。

Okta 表示，尽管黑客窃取了 Okta 的源代码，但并未访问 Okta 服务或客户数据。Okta 的“HIPAA，FedRAMP 或 DoD（国防部）客户”不受影响，因为 Okta 保护服务的手段“不依赖其源代码的机密性”。因此，无需其客户执行任何操作。

https://www.secrss.com/articles/50281

8、黑客出售 4 亿 Twitter 用户数据库

12 月 25 日报道，一名用户名 Ryushi 的用户在黑客论坛 Breached 兜售 4 亿 Twitter 用户的数据库，声称是利用 Twitter API 的漏洞抓取的，包括了电子邮件、用户名、姓名、粉丝数、创建日期和电话号码。

这位用户公开了几位名人的样本，排在最前面的是美国民主党议员 AOC（Alexandria Ocasio-Cortez）。黑客还建议 Twitter 或马斯克（Elon Musk）花钱购买该数据库，威胁他们将会面临因数亿用户数据被抓取而面临欧盟的 GDPR 巨额罚款，表示如果 Twitter 购买的话将会停止出售。

黑客利用的是今年早些时候已经修补的漏洞，上个月一个包含 540 万 Twitter 账号的数据库在黑客论坛免费共享，最新披露的数据规模则包含了绝大部分 Twitter 用户。

https://www.solidot.org/story?sid=73753

9、蔚来遭遇数据泄露，被勒索 225 万美元等额比特币

12 月 20 日，网络上有人称破解了蔚来大量数据，包括蔚来内部员工数据 22800 条、车主用户身份证数据 399000 条。

随后，蔚来官方发布《关于数据安全事件的声明》，称 2022 年 12 月 11 日，蔚来公司收到外部邮件，声称拥有蔚来内部数据，并以泄露数据勒索 225 万美元等额比特币。在收到勒索邮件后，公司当天即成立专项小组进行调查与应对，并第一时间向有关监管部门报告此事件。经初步调查,被窃取数据为 2021 年 8 月之前的部分用户基本信息和车辆销售信息。

https://c.m.163.com/news/a/HP20UCT8051191D6.html?from=wap_redirect&spss=adap_pc&referFrom=&spssid=7292497dc54ce3aa1a0cad4f280f9a2b&spsw=2&isFromH5Share=article

10、鞋类品牌 Ecco 在 500 天内泄露超 60GB 敏感数据

12 月 22 日消息，Cybernews 研究人员发现全球鞋类制造商和零售商 Ecco，在 500 天内暴露了数百万份敏感文件，共计 60GB。

Ecco 是一家丹麦鞋类制造商和零售商，在全球拥有数千家店铺和销售点。研究人员表示，不仅任何人都可能修改数据，而且服务器的配置错误很可能会使公司遭受攻击，从而波及世界各地的客户。

据了解，Ecco 从销售数据到系统信息的数百万份敏感文档都处于可在线访问状态，任何有权限的人都可以查看、编辑、复制、窃取或删除数据。

https://www.freebuf.com/articles/database/353229.html

11、体育博彩公司 BetMGM 披露数据泄露事件

12 月 22 日，据外媒报道，著名体育博彩公司 BetMGM 发生一起数据泄露事件，一名威胁攻击者成功窃取其未公开数量的大量用户个人信息。

据悉，BetMGM 数据泄露事件中，攻击者盗取了包括用户姓名、联系信息（如邮政地址、电子邮件地址和电话号码）、出生日期、加密的社会安全号码、账户标识（如 ID 和网名）

以及与 BetMGM 交易记录等了大量敏感数据信息。

虽然这家博彩公司尚未披露数据泄露事件中信息被盗的客户数量，但根据威胁行为者标题为“BetMGM.com 赌场数据库泄露”的帖子，被盗 BetMGM 客户信息的数据库据称包含 1,569,310 条用户记录。

https://www.bleepingcomputer.com/news/security/leading-sports-betting-firm-betmgm-discloses-data-breach/

12、俄罗斯黑客组织 Killnet 声称：已窃取 FBI 上万特工的个人数据

据 Hackread 网站 12 月 21 日报道，在 Telegram 上，知名的俄罗斯 Killnet 黑客泄露了一个文本文件，其中显示了他们声称是 FBI 特工的 10,000 人的登录凭据。该黑客组织还声称已经破坏了美国联邦汽车运输安全管理局(FMCSA)的安全措施。

据 KillNet 声称，其侵入了美国联邦调查局的数据库，窃取了超过 10,000 名美国联邦特工的个人信息。与他们的大多数攻击一样，这次所谓的攻击似乎也具有激励亲克里姆林宫组织的政治色彩。

尽管 Killnet 的攻击仍未得到证实，但 KillNet 黑客声称被盗数据包括社交媒体口令和银行详细信息。该组织在

Telegram 上发布了屏幕截图，其中显示了在线商店、医疗 ID 卡以及 Google、Apple 和 Instagram 帐户的口令。

https://www.secrss.com/articles/50267

13、LastPass 承认严重数据泄露，加密密码库被盗

12 月 23 日，据外媒报道，密码管理服务商 LastPass 透露，恶意行为者通过使用从早期入侵中窃取的数据，获得了属于其客户的大量个人信息，其中包括他们的加密密码库。

该公司表示，还被盗的还有“基本客户账户信息和相关元数据，包括公司名称、最终用户名称、账单地址、电子邮件地址、电话号码以及客户访问 LastPass 服务的 IP 地址”。LastPass 表示，身份不明的攻击者获得的凭据和密钥，随后被用来从存储在基于云的存储服务中的备份中提取信息，它强调该服务在物理上与其生产环境是分开的。最重要的是，据说攻击者已经从加密存储服务中复制了客户保险库数据。

https://thehackernews.com/2022/12/lastpass-admits-to-severe-data-breach.html?&web_view=true

14、德国连锁酒店 H-Hotels 遭 Play 勒索软件攻击，客户数据疑泄露

12 月 19 日，据外媒报道，近日，Play 勒索软件团伙发

表称对 H-Hotels (h-hotels.com) 进行了网络攻击，该攻击导致该公司通信中断。

H-Hotels 是一家国际连锁酒店企业，在德国、奥地利和瑞士的 50 个地点拥有 60 家酒店，客房总数超 9600 间。这家连锁酒店拥有 2500 名员工，是 DACH 地区最大的连锁酒店之一。

Play 勒索软件组织在声称对 H-Hotels 发动了攻击之后，在其 Tor 网站上列出了该公司，并称在网络攻击期间窃取了未公开数量的数据。这些数据包括私人和个人数据、客户文件、护照、身份证等。但是尚无任何证据表明他们真实的窃取了这些数据。

https://www.freebuf.com/news/353011.html

15、McGraw Hill 的 AWS S3 存储桶配置错误泄露 22TB 数据

据 12 月 19 日报道，研究人员发现了两个配置错误的 Amazon Web Services S3 存储桶，其所有者被确定为 McGraw Hill。该平台是美国三大教育内容出版商之一，也被加拿大各地的教育机构用于在线课程。此次事件总共泄露了 1.17 亿个文件，分别为一个包含 10TB 数据的非生产存储桶，以及一个包含 12TB 数据的生产存储桶，于 2022 年 6 月 12 日首次

被发现。研究人员透露，约 10 万名学生会受到该事件的影响，目前暴露的存储桶已被保护起来。

https://www.hackread.com/american-online-ed-platform-22tb-data-leak/

《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/