全球数据安全观察

总第 79 期 2022 年第 07 期

(2022.02.21-2022.02.27)

目录

政策形势	1
1、“东数西算”国家工程全面启动.....	1
2、工业领域数据安全试点地区名单公布.....	1
3、国务院：加强电子证照应用安全管理，严格保护信息安全.....	2
4、未成年人隐私保护，《上海市未成年人保护条例》3月1日起施行.....	3
5、上海市发布《中国（上海）自由贸易试验区临港新片区条例》，探索制定低风险跨境流动数据目录.....	4
6、上海首个“扫码点餐”规范指引发布，不得强取和过度收集个人信息.....	5
7、欧盟发布《数据法》草案.....	6
技术、产品与市场	7
1、微软洞察：身份管理漏洞成为数字安全首要威胁.....	7
2、Forrester：第三方风险管理市场将“百花齐放”.....	8
3、调查显示，零信任战略受到 CSO 好评.....	9
4、实现靠谱零信任的五个阶段.....	10
5、澳大利亚信息专员办公室：2021H2 464 起数据泄露....	10
业界观点	12
1、韦韬：迈进数据密态时代，拥抱可信隐私计算.....	12
2、邵志清：探索建立数据资产登记制度，积极参与国际数据	

治理.....	13
3、央行上海总部：任何人无权随意删除、修改征信记录，谨防诈骗.....	14
4、李翔：处理数据要有全流程合规意识.....	15
5、产业安全观智库邀专家探讨车企数据构筑云上安全防线的方案与思路.....	17
数据安全事件	18
1、芯片制造商巨头英伟达遭受勒索软件攻击.....	18
2、华硕子公司 ASUSTOR 遭攻击，被勒索上千万美元赎金.....	18
3、匿名者黑客组织攻击了俄罗斯国防部并针对俄罗斯公司.....	19
4、物流巨头 Expeditors 疑遭勒索软件攻击，全球业务关闭.....	19
5、炊具巨头 Meyer 披露了影响员工的网络攻击.....	20
6、医疗保健机构 Sea Mar 被指控数据泄露.....	20
7、尼日利亚黑客窃取工资存款.....	21
8、儿童奢侈品服装店 Melijoe 因云配置错误暴露 200 万个文件.....	22
9、答题赢“冰墩墩”，350 万人个人信息遭泄露.....	22
10、“颜值测试”黑客软件盗取超 8000 万条个人信息.....	23
11、西班牙/AEPD 对亚马逊公路运输公司非法处理刑事定罪数据罚款 200 万欧元.....	24

政策形势

1、“东数西算”国家工程全面启动

近日，国家发改委、中央网信办、工业和信息化部、国家能源局联合印发通知，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。至此，全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”中的“数”，指的是数据，“算”指的是算力，即对数据的处理能力。“东数西算”是通过构建数据中心、云计算、大数据一体化的新型算力网络体系，将东部算力需求有序引导到西部，优化数据中心建设布局，促进东西部协同联动。

<https://mp.weixin.qq.com/s/rQMSqPyAM8Q4a-0Vjc693Q>

2、工业领域数据安全试点地区名单公布

近日，工信部印发通知，部署做好工业领域数据安全管理工作，明确在辽宁等15个省（区、市）及计划单列市开展试点工作。要求各地工业和信息化主管部门认真学习贯彻《数据安全法》等法律法规、工业和信息化领域数据安全相关管理制度等要求，明确数据安全管理部门和负责人，指导本地区工业企业开展数据安全管理工作。

根据工信部此前印发的《关于组织开展工业领域数据安全管理工作试点工作的通知》，试点内容分为必选和可选两部分。必选试点内容包括：工业领域数据安全管理工作、工业领域数据安全产品应用推广、工业领域数据安全监测、工业领域数据出境安全管理。

<https://mp.weixin.qq.com/s/MVfN6JYwLrlqVFyLRRGODA>

3、国务院：加强电子证照应用安全管理，严格保护信息安全

国务院办公厅近日发布了《关于加快推进电子证照扩大应用领域和全国互通互认的意见》。《意见》共五章十八条，包括总体要求、扩大电子证照应用领域、推动电子证照全国互通互认、全面提升电子证照应用支撑能力和保障措施。

其中强调加强电子证照应用安全管理和监管。加强电子证照签发、归集、存储、使用各环节安全管理，严格落实网络安全等级保护制度等要求，强化密码应用安全性评估，探索运用区块链、新兴密码技术、隐私计算等手段提升电子证照安全防护、追踪溯源和精准授权等能力。按照信息收集最小化原则归集数据，对共享的电子证照进行分类分级管理，避免信息泄露。加快推进国家网络身份认证公共服务基础设施建设和应用，加强对电子证照持证主体、用证人员的身份

认证、授权管理和个人信息保护。强化企业和群众身份认证支撑，增强电子证照签发和使用等环节的统一身份认证能力。建立健全严格的责任追究制度，依法严厉打击电子证照制作生成过程中的造假行为，杜绝未经授权擅自调用、留存电子证照信息，切实保障电子证照及相关信息合法合规使用，保护持证主体的商业秘密和个人信息。

<https://mp.weixin.qq.com/s/RyC4LYHuPhPcqPi8ujqTVA>

4、未成年人隐私保护，《上海市未成年人保护条例》3月1日起施行

2月18日，上海市十五届人大常委会第三十九次会议上表决通过了《上海市未成年人保护条例》，将于2022年3月1日起施行。《条例》共九章八十七条，涵盖了家庭保护、自我保护、学校保护、社会保护、网络保护、政府保护、司法保护、特别保护等内容。

围绕未成年人的个人信息保护及网络保护，《条例》进行了相应的规定。包括：任何组织或者个人不得披露未成年人的个人隐私。发布、转载、传播涉及未成年人的新闻报道等信息，应当客观、审慎和适度，不得虚构、夸大、歪曲有关内容，不得违法披露未成年人的姓名、住所、单位、照片、图像以及其他可能识别未成年人身份的信息。任何组织或者

个人处理不满十四周岁未成年人个人信息的，应当依法取得未成年人的父母或者其他监护人的同意。未成年人的父母或者其他监护人应当按照最有利于未成年人的原则，充分考虑信息处理的目的、方式、范围以及未成年人的真实意愿，审慎作出决定。

<https://mp.weixin.qq.com/s/4AhTvwm65JyQW1c3w-jKRA>

5、上海市发布《中国（上海）自由贸易试验区临港新片区条例》，探索制定低风险跨境流动数据目录

2月18日，上海市十五届人大常委会第三十九次会议高票表决通过了《中国（上海）自由贸易试验区临港新片区条例》，并且将于3月1日正式实施。《条例》完善了特殊经济功能区建设的四梁八柱，设总则、投资自由便利、贸易和运输自由便利、资金自由便利、人员从业自由便利和人才保障、数据流动、前沿产业发展、风险防范、权益保障、附则共十章五十五条。

其中强调，按照国家相关法律、法规的规定，在临港新片区内探索制定低风险跨境流动数据目录，促进数据跨境安全有序流动。支持临港新片区推进国际数据产业发展，培育发展数据经纪、数据运营、数据质量评估等新业态，建立数据跨境流动、数据合规咨询服务、政企数据融合开发等公共

服务平台。

<https://mp.weixin.qq.com/s/9MqPtRjATwdQkpoa3grHPA>

6、上海首个“扫码点餐”规范指引发布，不得强取和过度收集个人信息

2月23日，上海首个《餐饮行业“扫码点餐”规范指引》正式发布，引导经营者对相关行为进行规范。《指引》明确，餐饮服务经营者收集消费者信息应当遵循合法、正当、必要的原则，在提供扫码点餐服务时，应当限于实现处理目的的最小范围，不得强制要求消费者对手机号、微信号等个人信息进行注册或授权，不得过度收集消费者信息。餐饮服务经营者通过折扣或优惠的方式吸引消费者注册或授权的，应当单独取得消费者同意，不得与扫码点餐服务捆绑。连锁餐饮服务行业各门店之间共享消费者个人信息的，应当向消费者告知共享范围并明确取得消费者同意。

《指引》明确，餐饮服务经营者对已收集的消费者信息必须严格保密，不得泄露、出售或者非法向他人提供；未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。对于经营者违法收集消费者个人信息的，市场监管部门将按照《消费者权益保护法》等法律法规进行查处。

<https://mp.weixin.qq.com/s/W5uFEUtotGEgryWTkFMycw>

7、欧盟发布《数据法》草案

2月23日，欧盟公布了《数据法》草案全文，该草案旨在为数据共享、公共机构的访问条件、国际数据传输、云转换和互操作性提供一个统一的法律框架，其核心目标是使用户和供应商在获取数据方面处于更加平等的地位。具体来说，每一个对数据产生有贡献的行为者都能访问上述数据。

《数据法》还将要求企业引入保护措施，阻止非欧盟政府访问数据，并强制企业允许用户在云提供商之间免费传输数据。欧洲数据法案超越了目前对个人数据转移到欧盟以外的限制，将这种限制扩大到非个人数据。只有在达成国际协议的情况下，来自第三国的法院命令才会被遵守。《数据法》规定了某些限制，以保证第三方对共享数据的访问对有关各方都是安全 and 无害的。这需要采取商定的措施来保护机密性、隐私和商业秘密，以及限制数据持有人的市场竞争对手使用数据。

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

技术、产品与市场

1、微软洞察：身份管理漏洞成为数字安全首要威胁

确保身份认证及管理的安全性是确保数字安全的中中之重。当今世界，身份认证已经成为关乎每个人工作生活方方面面的关键凭证，“身份”背后存储的是每个人在浩如烟海的各类应用和服务中的全部记录。正是因为身份认证如此重要，如果没有对身份认证加以正确的安全保护，将带来巨大的潜在风险。目前以多因素认证（MFA）、无密码方案为代表的强身份认证的使用率还很低——而那些仅仅依靠密码保护的账号，常常成为黑客们最容易得手的目标。

微软数据显示，截至 2021 年 12 月，在采用微软云端身份解决方案 Azure Active Directory (AAD) 的各行业客户中，只有 22% 启用了强身份认证保护措施。仅在 2021 年 1 月到 12 月的一年里，微软就阻止了 256 亿次针对 AAD 的暴力破解身份认证攻击，并通过 Microsoft Defender for Office 365 拦截了 357 亿封网络钓鱼电子邮件。

对于大多数组织来说，以多因素认证、无密码解决等方案强化身份管理，是防范各种类型安全威胁，最行之有效又简便易行的重要手段。企业和组织可以通过以下方式更好地保护自己：（1）启用多因素身份验证（MFA）；（2）审核

账户权限；(3)审查、强化和监视所有租户管理员账户；(4)建立并实施安全基线以降低风险。

<https://www.freebuf.com/articles/323039.html>

2、Forrester: 第三方风险管理市场将“百花齐放”

研究咨询公司 Forrester 在最新发布的《Now Tech: 第三方风险管理平台, 2022 年第一季度》报告中称, 第三方风险管理 (TPRM) 在业务优先级和风险管理优先级列表中位居前列, 并将呈现“百花齐放”的发展态势。

目前, 有几类供应商支撑 TPRM 市场, 每一类专注于一个或多个风险领域、行业或客户成熟度级别。Forrester 的新报告《Now Tech: 第三方风险管理平台, 2022 年第一季度》, 根据功能将 22 种主要的 TPRM 技术分为四大类, 每一大类都有适合不同类型买家的供应商。

(1) 专用技术。这类技术在整个第三方风险管理生命周期当中提供强大功能。它们结合领域专业知识和广泛功能, 以支持所有级别的 TPRM 成熟度。

(2) GRC 平台。治理、风险和合规 (GRC) 平台为众多的风险和合规使用场景提供强大支持。

(3) 风险信息交换中心。风险信息交换中心让组织可以访问预先填好和验证的评估结果、多种类型的文档和证据以

及分析工具。

(4) 专注于垂直领域的供应商。这些提供商拥有扎实的专业技术专长、GRC 平台的广泛功能, 并经常提供支持服务, 但尤其关注第三方合规要求很复杂的行业。

<https://www.secrss.com/articles/39235>

3、调查显示, 零信任战略受到 CSO 好评

Optiv 发布了一份基于网络安全领导者的调查报告, 该报告着重强调了实施零信任是降低网络风险有效方式的重要性。

报告概括了来自 150 个不同行业、不同部门的调查答复, 主要包括金融、医疗保健、高科技和政府等, 43% 的受访对象在 1000-5000 名员工规模的组织内担任 CISO/CSO 职位。

受访者普遍认为零信任是最有效的安全实践之一, 100% 的受访者承认零信任对降低其组织的网络风险非常重要。

Optiv 工程研究员 Jerry Chapman 称: 实施零信任战略的必要性和重要性是网络安全领导者的首要考虑。

<https://www.freebuf.com/news/322010.html>

4、实现靠谱零信任的五个阶段

零信任方法的主要目标是从“信任，但验证”，转向“验证，然后信任”。我们不应隐式信任所有实体，而应该持续评估上下文。零信任的次要目标是假设业务环境随时会遭破坏，并以此为前提逆向设计安全防护方案。通过消除隐式信任，通过基于身份、自适应访问和综合分析持续评估用户和设备置信度，零信任方法可以降低风险并提高业务敏捷性。

各家公司实现零信任的旅程可能并不完全相同，但总的说来可分为以下五个关键阶段：

阶段 1：禁止匿名访问；

阶段 2：维护显式信任模型；

阶段 3：实施隔离，限制影响范围；

阶段 4：实现持续数据保护；

阶段 5：通过实时分析和可视化加以完善。

<https://mp.weixin.qq.com/s/pPbOfv0XfPCYizKvBA0eOA>

5、澳大利亚信息专员办公室：2021H2 464 起数据泄露

私营医疗服务行业再次成为澳大利亚上报数据泄露事件数量最多的行业，2021 年澳大利亚信息专员办公室(OAIC)接到的所有数据泄露报告中有 18%出自这个行业。

去年上半年，OAIC 共收到 464 起数据泄露报告，与 2021

年上半年相比增加了 6%。私营医疗服务提供商贡献了其中 83 起。金融领域次之，报告了 56 起；法律、会计和管理服务行业则以 51 起位列第三。

恶意或犯罪攻击仍是数据泄露的主要源头，共 256 起数据泄露事件源自于此。同时，人为失误引发的数据泄露大幅增加了 43%，达到 190 起。而系统故障则占去年下半年数据泄露事件根源的 4%。

细分人为失误型数据泄露的几种主要原因：其中 43%是由于个人信息发送到了错误的邮箱，21%是意外泄露，而 8%是由于丢失了文书或数据存储设备。

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

业界观点

1、韦韬：迈进数据密态时代，拥抱可信隐私计算

隐私计算成为解决数据安全和个人信息保护这一挑战的核心技术。近日，蚂蚁集团副总裁，蚂蚁集团安全隐私科技委员会主席，北京大学客座教授韦韬对数据要素行业正在到来的“密态时代”的特性、技术挑战和技术方向发表了详细阐述。

韦韬表示，面对数据要素发展和数据安全保护的双诉求，数据密态无疑是当前最好的选择。一方面，运营者要想“确保其收集的个人信息安全”，最简单有效的就是保证其数据明文不被其他方获得；另一方面，《个人信息保护法》规定了经过匿名化的信息不再受“授权墙”制约，但明文的匿名化数据会丢失个体粒度的信息，也就是说，如果要保持数据价值，匿名化后的数据也需要进行密态化处理。

韦韬认为，数据密态技术一定要达到作为广泛性业务基础设施的技术门槛要求，才能满足数据密态时代的要求，包括五点：性能要足够高，足够稳定，成本足够低，适用性足够广，安全性足够高且达成行业共识。

同时，韦韬提出：隐私计算往前走、进一步落地给产业，并满足合规要求，非常重要的方向是“可信隐私计算”。他

认为，可信隐私计算的核心是在隐私计算的技术体系以及技术实现层面提供可信支撑，对个人信息和敏感数据提供高效的、全生命周期的安全合规保障。业界可以在可信隐私计算的框架下有效的解决当下面临的合规、业务支撑、安全适用等挑战。

<https://mp.weixin.qq.com/s/6BPzs2Tarsek-iBF8rJAtA>

2、邵志清：探索建立数据资产登记制度，积极参与国际数据治理

今年即将召开的全国两会上，全国人大代表、致公党上海市委专职副主委邵志清将提交《关于制定数据资产登记法的议案》：“建立新时代中国特色数据资产登记制度体系和技术标准体系，汇聚全国有价值的数据要素资源和数据资产，构建我国数据资源底座，服务经济发展、社会治理，也引领全球数字经济发展。”

在邵志清看来，为数据资产确认权属，是释放数据要素价值、推动数据要素流通，必须跨过的第一道坎。如果数据资产也能有一本自己的权威登记证书，将数据来源、提供者、权利人、使用期限、使用次数、使用限制、安全等级、保密要求等作为事实确认下来，“就是打开了定价、入场、监管等后续环节的链路开端”。

“随着我国要素市场化配置综合改革进程不断推进，迫切需要通过制定数据资产登记法来解决上述问题。”邵志清认为，应当立法制定包括数据资产目录、样本、交换接口、质量评估、来源及其内容合规性评估等方面的关键共性技术规范、系统标准和互连标准，形成完善的围绕数据资产价值化的数据登记和产业创新生态体系。

https://mp.weixin.qq.com/s/CjvI21nQXrEf6O1f46p_oA

3、央行上海总部：任何人无权随意删除、修改征信记录，谨防诈骗

近年来，一些不法分子打着“征信修复”“征信洗白”的旗号，教唆信息主体委托其办理征信投诉、举报等事项，以此牟取不正当利益，扰乱正常金融秩序。中国人民银行上海总部向广大市民郑重提示：“征信修复”不可信。

人民银行上海总部有关人士介绍，目前“征信修复”主要有三种套路：一是收取高额费用后跑路，二是征信培训、加盟诈骗，三是骗取个人敏感信息。

对此，人民银行上海总部有关人士强调：“征信领域不存在‘修复’‘洗白’等说法，凡是声称合法的、收费的‘征信修复’都是骗局，任何人都无权随意删除、修改征信记录。”同时表示，“如果市民认为信用报告上的个人信息存在错误、

遗漏，可以向金融机构或人民银行征信中心提出异议，办理异议不收费。如果市民认为自己的征信合法权益被侵害，也可以到本地的人民银行分支机构进行投诉，投诉也是免费的。”

<https://mp.weixin.qq.com/s/cA-fF3aRqhA5Dtd9YTmCpQ>

4、李翔：处理数据要有全流程合规意识

近日，一科技公司利用爬虫技术窃取 2.1 亿条简历数据，被告人被追究刑事责任。该科技公司主要经营招聘工具软件和大数据分析等业务，组建有专门的爬虫技术团队，在未取得求职者和平台授权的情况下，秘密爬取了国内主流招聘平台上的大量求职者简历数据。获取数据后，公司对数据进行重整，用于开发产品意图谋利。其间，该公司爬虫技术团队负责人还私自将简历数据对外出售，非法获利人民币 30 余万元。最终被告单位被处罚金 4000 万元，被告人王某某判处有期徒刑 7 年，并处罚金 1000 万元，其他被告人均被判处相应刑罚。

华东政法大学刑事法学院教授、博士生导师李翔表示，近年来，利用爬虫技术实施违法犯罪的案例屡见不鲜，企业进行数据处理时，应当与时俱进，走出以往数据处理的观念误区。他指出，虽然爬虫技术本身并不违法，但是企业在利

用爬虫技术采集个人信息时，要注意不得妨碍被采集网站的正常运营，不得违背个人信息主体的意愿。

李翔表示，数据处理包含收集、存储、使用、加工、传输、提供、公开等全流程，企业应走出数据处理仅是防止泄露的误区。此案之所以是近期类似案例中被处罚较严重的案件，除了涉及个人信息数据量较大外，恐怕也跟该公司在数据处理的多个环节均存在违反法律规定的行为有关。比如，在数据收集环节，利用爬虫技术大规模采集求职者简历数据，未取得求职者和平台的授权；在数据存储环节监管失当，致使员工私自将简历数据对外出售，导致大量数据被泄露；在数据使用、加工等环节，对收集来的数据进行重整并用于开发产品意图谋利。

此外，李翔表示数据处理要形式合规与实质合规并重，企业应走出形式化合规的误区。例如在此案中，涉案公司员工私自将求职者简历数据出售获利，就暴露出该公司在数据存储环节缺乏必要的监管。总而言之，数据合规并不是独立于企业管理和产品之外的体系，企业应当将数据合规与企业管理、生产及服务流程有机融合，进而实现企业经营的合法合规。

http://www.china.com.cn/opinion/think/2022-02/23/content_78066467.htm

5、产业安全观智库邀专家探讨车企数据构筑云上安全防线的方案与思路

产业安全观智库访谈邀请到上海帆一尚行科技有限公司网络安全总监、上汽腾讯网络安全实验室联合负责人陈宁和腾讯安全策略发展中心总经理吕一平，围绕汽车数据安全和风险防御问题展开详细解读，共同探讨车企数据构筑云上安全防线的方案与思路。

陈宁表示，汽车联网以后，对于汽车的各类服务如自动驾驶等，是不可避免要搜集很多数据的。分类数据时，首先要按照服务的细分分类，其次要注意数据的共享和流动。这也是很重要的因素，现在很多服务在云上之后，不仅主机厂要收集数据，车企的合作伙伴等也需要收集数据。在数据流通过程中，车企该如何对数据进行授权、约束，以及以什么样的合法合规方式流通，都是需要处理的。

吕一平提出，国家在出台安全合规性要求越来越快，能给车企应对的时间非常紧张。这种情况下快速地建立安全能力很重要。目前我们能看到一个挑战是，在汽车行业数字化投入中，网络安全部分的投入只有2%到3%左右，而相较之下，经历了二十年IT能力建设的金融行业，网络安全投入大概8%到10%。可见加大投入是可以加速能力建设的。

<https://mp.weixin.qq.com/s/okdcNhIRQC2ZNIQJMPLqeA>

数据安全事件

1、芯片制造商巨头英伟达遭受勒索软件攻击

2022 年 2 月 27 日报道，芯片制造商巨头英伟达遭受了勒索软件攻击，该攻击影响了其部分系统达两天。Lapsus \$ 勒索软件团伙声称对这次攻击负责，该组织宣布从英伟达的网络中窃取了 1 TB 的数据。勒索软件团伙泄露了所有英伟达员工的在线凭证。

<https://securityaffairs.co/wordpress/128456/cyber-crime/nvidia-ransomware-attack.html>

2、华硕子公司 ASUSTOR 遭攻击，被勒索上千万元赎金

2022 年 2 月 24 日，据报道，华硕旗下子公司华芸科技（Asustor）的网络附加存储（NAS）也遭遇了勒索攻击。此次勒索攻击波及全球众多用户，并在 ASUSTOR 论坛上引起广泛讨论。

两次攻击均是 DeadBolt 勒索软件所为，所有文件都被加了 .deadbolt 文件扩展名。ASUSTOR 登录页面也被一张数据勒索通知代替，要求用户支 0.03 个比特币，折合人民币约七千多元。

<https://www.freebuf.com/news/323073.html>

3、匿名者黑客组织攻击了俄罗斯国防部并针对俄罗斯公司

2月26日，据报道，全球最大的黑客组织“匿名者 (Anonymous)”宣布对俄罗斯发起“网络战争”，并声称对“今日俄罗斯” (RT) 遭受的一次网络攻击负责。据《真理报》报道，匿名者成功入侵并泄露了俄罗斯国防部网站的数据库。匿名者也在对那些支持乌克兰军事行动的国家发起攻势，比如白俄罗斯。该组织还泄露了来自白俄罗斯武器制造商 Tetraedr 的约 200GB 电子邮件。这家公司为普京入侵乌克兰提供了后勤支持。

<https://securityaffairs.co/wordpress/128428/hacking/anonymous-russian-defense-ministry.html>

4、物流巨头 Expeditors 疑遭勒索软件攻击，全球业务关闭

2022年2月17日，联邦调查局警告说，俄罗斯国家支持的特工正在瞄准美国承包商网络以获取敏感的国防信息，其中一些人获得了至少六个月的持续访问权。

美国网络安全和基础设施安全局 (CISA) 16日发布的一份声明详细说明了它如何观察到2020年1月至2022年2月期间美国已获批准的国防承包商 (CDC) 的“常规目标”。CISA表示，在两年的时间里，俄罗斯参与者保持对多个 CDC 网络的持续访问，在某些情况下至少持续六个月。

FBI、NSA 和 CISA 注意到电子邮件和数据的定期和反复泄露。

<https://portswigger.net/daily-swig/russian-nation-state-hackers-targeting-us-contractors-for-sensitive-defense-information-fbi-warns>

5、炊具巨头 Meyer 披露了影响员工的网络攻击

2022 年 2 月 21 日报道，美国最大的炊具分销商、全球第二大炊具分销商 Meyer Corporation 已向美国司法部长办公室通报了影响其数千名员工的数据泄露事件。

相关调查显示，威胁行为者获得了属于 Meyer 及其子公司员工的个人信息的访问权限，可能已经暴露和复制的个人信息包括以下内容：姓名、地址、出生日期、社会安全号码、健康保险信息、护照等等。

<https://www.bleepingcomputer.com/news/security/cookware-giant-meyer-discloses-cyberattack-that-impacted-employees/>

6、医疗保健机构 Sea Mar 被指控数据泄露

2022 年 2 月 22 日，据外媒报道，一家位于西雅图的医疗保健机构 Sea Mar 社区健康中心因网络攻击而面临集体诉讼，其中 688,000 人的受保护健康信息被泄露。

网络犯罪团伙 Marketo 将攻击中被盗的文件在暗网上公开,其声称从 Sea Mar 窃取了 3TB 数据。Sea Mar 表示,黑客在 2020 年 12 月至 2021 年 3 月期间获得了对其网络的访问权限,网络犯罪分子利用该访问权限窃取了敏感数据,包括姓名、出生日期、健康信息、地址和社会安全号码。

<https://www.infosecurity-magazine.com/news/sea-mar-negligence-data-breach/>

7、尼日利亚黑客窃取工资存款

2022 年 2 月 23 日报道,一名名叫查尔斯·奥努斯(Charles Onus)的尼日利亚国民在纽约南区地方法院承认侵入一家人力资源和薪资公司的用户账户并窃取工资存款。威胁者使用撞库攻击来访问该公司的账户,该公司负责为其他公司的员工支付工资。

根据起诉书和法庭上的陈述, Onus 积极参与了一项计划,该计划接管了美国各地公司员工的用户账户,并通过将工资转移到他控制的借记卡上来窃取工资存款。

这种恶意活动始于 2017 年 7 月,在他被捕之前, Onus 已经入侵了 5,500 个用户帐户,转移了总计 80 万美元的工资资金。

<https://www.bleepingcomputer.com/news/security/nigerian->

[hacker-pleads-guilty-to-stealing-payroll-deposits/](#)

8、儿童奢侈品服装店 Melijoe 因云配置错误暴露 200 万个文件

2022 年 2 月 21 日报道，Melijoe 是一家总部位于法国的高端儿童时装零售商，该公司所拥有的一个 Amazon S3 存储桶在没有适当的身份验证控制的情况下仍然可以访问，从而暴露了数十万客户的敏感数据和个人身份信息 (PII)。

经调查，错误配置的 Amazon S3 存储桶暴露了近 200 万个文件，总计约 200 GB 的数据，这些文件包含不同的数据集：偏好、愿望清单和购买记录。暴露的客户 PII 和敏感数据包括：电子邮件地址、儿童姓名、性别、出生日期、品牌偏好、帐单地址等等。除了上述数据，Melijoe 的存储桶还包含有关 Melijoe 的产品目录和库存水平的信息。

https://www.safetydetectives.com/news/melijoe-leak-report/?&web_view=true

9、答题赢“冰墩墩”，350 万人个人信息遭泄露

2022 年 2 月 23 日报道，趁着冬奥会热潮，一场以“冬奥知识传播”线上答题活动为幌子的骗局在网上传播开来。很多大中专院校学生冲着活动主办方承诺的冬奥大使荣誉

证书、“冰墩墩”手办参与答题，却因此泄露了姓名、身份证号、手机号、所在学校等个人信息，目前涉案学生人数已达 350 余万名。

<https://mp.weixin.qq.com/s/FuKblbtSSwn1rwtitbkHZQ>

10、“颜值测试”黑客软件盗取超 8000 万条个人信息

2022 年 2 月 24 日，据央视新闻报道，近日在上海司法机关办理的一起泄露个人信息案件中，显示与一款颜值打分软件有关。

这款涉案的颜值打分软件。它声称可对脸部照片自动评分，还能判断肌肤状态。但实际上，这款软件被人安装之后，它会获取被安装的人的手机照片传到不法分子的服务器上。被告人李某通过将这款所谓的颜值打分软件上传到网络上供网民免费使用的方式，先后窃取了 1700 多张用户照片，其中比较完整的公民个人信息有 100 多条。而除此之外，李某还将这个软件发布在了一个隐藏的暗网论坛上进行售卖，其虚拟货币流向牵出一个包含着 8100 多万条个人信息的“社工库资料”买卖。

https://mp.weixin.qq.com/s/ISKikd_-34MaYJSRk31csg

11、西班牙/AEPD 对亚马逊公路运输公司非法处理刑事定罪数据罚款 200 万欧元

西班牙数据保护局 (AEPD) 公布对亚马逊公路运输西班牙有限公司处以 200 万欧元罚款。因为其在雇佣承包商时要求候选者提供犯罪记录并同意数据传输的行为违反了 **GDPR 第 6 (1) 条和第 10 条**，以及 **2018 年 12 月 5 日关于保护个人数据和保障数字权利的第 3/2018 号组织法 (LOPDGDD) 第 10 条**。

https://mp.weixin.qq.com/s/7VYBfJEyZ3ZR_Bjh17nQ2A