

全球数据安全观察

总第 95 期 2022 年第 23 期

(2022.06.27-2022.07.03)

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、国家网信办发布《互联网用户账号信息管理规定》，8月1日起施行.....	1
2、关于《个人信息出境标准合同规定（征求意见稿）》公开征求意见的通知.....	2
3、《中华人民共和国反电信网络诈骗法（草案二次审议稿）》发布.....	2
4、全国首部！《深圳经济特区智能网联汽车管理条例》通过，重点规范网络安全和数据保护.....	3
5、美议员提出《2022 保护美国数据免受外国监视法案》..	4
技术、产品与市场	6
1、信通院发布 2022 年大数据十大关键词.....	6
2、机密计算在国际市场高速发展，以可信执行环境为核心的机密计算成为隐私计算赋能领域重要的解决方案.....	7
3、我国数字经济规模超 45 万亿元.....	8
4、IDC：2021-2026 年中国数字化转型市场预测.....	8
5、勒索软件数量在一个季度内几乎翻了 2021 年的总量...9	9
业界观点	11
1、解读与建议：关于开展数据安全认证工作的公告..	11
2、杜跃进：数字安全进入能力主义时代.....	12

3、沈浩：大数据视域下的数据伦理与消费者保护	14
4、刘典：构建数据基础制度安全网	15
5、知网突遭审查，孔德亮：数据安全关乎国家安全，合规是 生命线.....	16
数据安全事件	18
1、RansomHouse 团伙声称从芯片制造商巨头 AMD 窃取了 450GB 数据	18
2、密苏里州菲茨吉本医院遭勒索软件攻击，敏感数据泄露	18
3、沃尔玛拒绝承认遭 Yanluowan 勒索软件攻击.....	19
4、Carnival Cruises 因数据泄露事件被罚款 125 万美元	20
5、工行收集与业务无关的消费者金融信息等，被罚 618.7 万 元.....	20
6、Cyble 称有超过 90 万个配置错误的 Kubernetes 暴露在网上.....	21
7、加利福尼亚州的枪支管制网站暴露个人数据	21
8、OpenSea 披露数据泄露，警告用户网络钓鱼攻击	22

政策形势

1、国家网信办发布《互联网用户账号信息管理规定》，8月1日起施行

6月27日，国家互联网信息办公室发布《互联网用户账号信息管理规定》（以下简称《规定》），自**2022年8月1日起施行**。国家互联网信息办公室有关负责人表示，出台《规定》，旨在加强对互联网用户账号信息的管理，弘扬社会主义核心价值观，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，促进互联网信息服务健康发展。

《规定》明确，互联网用户账号信息是指互联网用户在互联网信息服务中注册、使用的名称、头像、封面、简介、签名、认证信息等用于标识用户账号的信息；互联网信息服务提供者，是指向用户提供互联网信息发布和应用平台服务的主体。国家网信部门负责全国互联网用户账号信息的监督管理工作。地方网信部门依据职责负责本行政区域内的互联网用户账号信息的监督管理工作。

此外，《规定》还明确了账号信息注册和使用规范、账号信息管理的规范以及开展监督检查和追究法律责任的相关要求。

http://www.cac.gov.cn/2022-06/26/c_1657868775333429.htm

2、关于《个人信息出境标准合同规定（征求意见稿）》公开征求意见的通知

为了规范个人信息出境活动，保护个人信息权益，促进个人信息跨境安全、自由流动，依据《中华人民共和国个人信息保护法》，国家互联网信息办公室起草了《个人信息出境标准合同规定（征求意见稿）》（简称“规定”），于06月30日向社会公开征求意见。

规定中明确了可以通过签订标准合同的方式向境外提供个人信息的情形、标准合同的主要内容、备案流程等要求，并在附件中提供了《个人信息出境标准合同》文本。

http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm

3、《中华人民共和国反电信网络诈骗法(草案二次审议稿)》发布

近日，《中华人民共和国反电信网络诈骗法（草案二次审议稿）》发布（以下简称《反电信网络诈骗法》）。《反电信网络诈骗法》共七章四十六条，将有利于进一步预防、遏制和惩治电信网络诈骗活动,加强反电信网络诈骗工作,保护公民和组织的合法权益,维护社会稳定和国家安全。

《反电信网络诈骗法》指出，“电信网络诈骗”是指以非

法占有为目的，利用电信网络技术手段，通过远程、非接触方式，诈骗公私财物的行为。

针对电信行业，《反电信网络诈骗法》指出，电信业务经营者应当依法落实电话用户真实身份信息登记制度。国务院电信主管部门组织建立电话用户开卡数量核验机制和风险信息共享机制,并为用户询名下电话卡信息提供便捷渠道。

针对金融行业，《反电信网络诈骗法》指出，银行业金融机构、非银行支付机构为客户开立银行账户、支付账户等支付工具及提供支付服务,和与客户业务关系存续期间，应当建立客户尽职调查制度，依法识别受益所有人，采取相应风险管理措施，防范银行账户、支付账户等被用于电信网络诈骗活动。

针对互联网治理，《反电信网络诈骗法》指出，电信业务经营者、互联网服务提供者在与用户签订协议或者确认提供服务时，应当依法要求用户提供真实身份信息，明确规定了用户不提供真实身份信息的，不得提供的服务范围。

<https://www.freebuf.com/news/337401.html>

4、全国首部!《深圳经济特区智能网联汽车管理条例》通过，重点规范网络安全和数据保护

6月23日，《深圳经济特区智能网联汽车管理条例》（征

征求意见稿)》获市七届人大常委会第十次会议表决通过。条例出台后,将有力推动深圳市智能网联汽车产业迈上新台阶。征求意见稿说明中提到,网络安全和数据保护是智能网联汽车立法需要重点规范的内容。意见稿提到,市互联网信息部门应当对智能网联汽车产品、服务及其供应链存在的网络安全风险进行监督管理。智能网联汽车相关企业应当按照市互联网信息部门的要求取得网络安全检测认证,依法建立网络安全评估及管理机制;应当依照国家相关规定,采取措施防止用户个人信息的泄露、丢失、损毁,并制定数据安全及隐私保护方案。禁止非法收集、处理、利用个人隐私、信息,禁止非法采集涉及国家安全的数据。

https://mp.weixin.qq.com/s/bBEHZq_jjIZOILswo53aaQ

5、美议员提出《2022 保护美国数据免受外国监视法案》

6月23日,美国参议员 Ron Wyden 与 Sheldon Whitehouse、Cynthia Lummis、Marco Rubio、Bill Hagerty 一起提出了《2022 保护美国人数据免受外国监视法案》(The Protecting Americans' Data from Foreign Surveillance Act of 2022),以控制将某些敏感类别的美国公民数据共享和传输给被视为国家安全风险的外国实体。该法案目前已被提交至参议院委员会。

此前，6月15日，美国参议员 Elizabeth Warren 提出了《健康和位置数据保护法》（Health and Location Data Protection Act），禁止数据经纪人出售美国人的位置和健康数据。

以上两项法案都针对庞大的数据经纪生态系统，在这个生态系统中，美国公司收集、汇总、分析、打包并提供数百万美国人的数据。这一生态系统对公民权利、消费者隐私、人身安全和国家安全造成的危害，需要立即进行监管。特别是对特定社群造成的伤害，从警力密集的黑色和棕色人种社区，到穷人、老年人、家庭暴力幸存者，再到患有创伤后应激障碍的退伍军人。虽然国会必须通过一项全面的消费者隐私法，但立法者没有理由允许当前数据经纪人的危害继续下去。

<https://www.secrss.com/articles/44075>

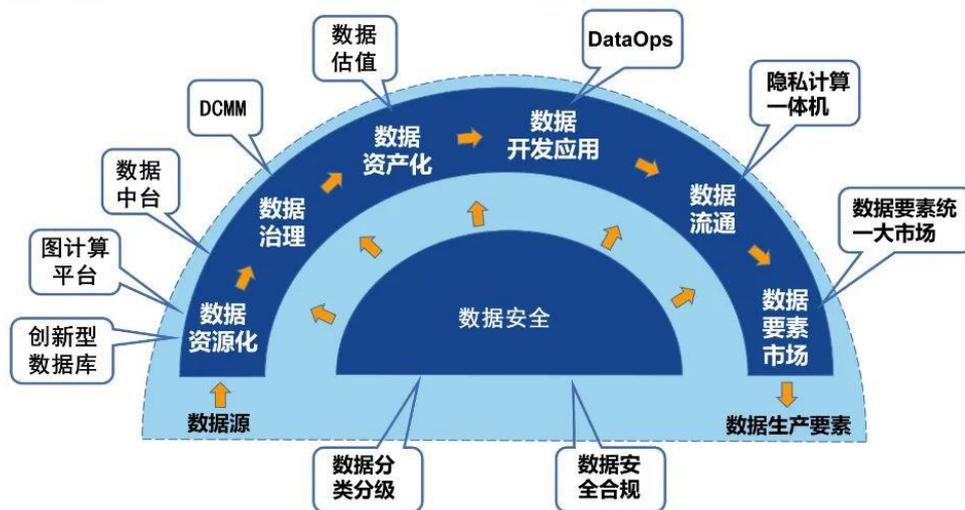
技术、产品与市场

1、信通院发布 2022 年大数据十大关键词

2022 大数据产业峰会，信通院基于长期对于产业的研究观察，以及与一线专家的研讨交流发布了《2022 大数据十大关键词》。

2022大数据十大关键词总览

BIG DATA
INDUSTRY 大数据产业峰会
CONFERENCE 2022
开启数据化新篇章



如图所示，本年度十大关键词涉及数据从计算机语言到成为生产要素的全生命周期，包括（1）【数据资源化】，即数据从计算机语言到成为可被人类识别的信息（2）【数据治理】，即将散乱的、庞杂的数据进行归类、整理、管理（3）【数据资产化】，即将数据与货币进行对应挂钩，（4）【数据开发应用】，即加工数据使其为业务赋能，（5）【数据流通】，即完成数据在部门与部门间、机构与机构间进行点对

点的合规交换共享，（6）【数据要素市场】，即促进全社会按照统一规范的制度、体系完成数据的合规流通利用，（7）【数据安全】，即保障数据流转的全生命周期符合相关法律法规。

<https://www.secrss.com/articles/44086>

2、机密计算在国际市场高速发展，以可信执行环境为核心的机密计算成为隐私计算赋能领域重要的解决方案

大数据时代，数据流通、安全等问题接踵而至，基于 CPU 可信执行环境的机密计算技术可以在保证数据“可用而不可见”的前提下进行数据运算，成为解决数据流通安全问题的热点技术。根据国外著名信息调查机构 Everest Group 最近的一项市场研究表明，**机密计算市场预计将在 5 年内增长到 54 亿美元。**

Everest Group 的市场调研中显示，2021 年，机密计算的可触达市场空间（TAM）为 19-20 亿美元。预计到 2026 年，机密计算市场在理想的情况下将以 90-95% 的年复合增长率增长，在不理想的情况下至少以 40-45% 的年复合增长率增长。其中在 2021 年超过 75% 的需求受到银行、金融和医疗保健等受监管行业的推动。

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

3、我国数字经济规模超 45 万亿元

据从工业和信息化部近日消息：近年来，我国数字经济蓬勃发展，产业规模持续快速增长，已数年稳居世界第二。统计测算数据显示，从 2012 年至 2021 年，我国数字经济规模从 11 万亿元增长到超 45 万亿元，数字经济占国内生产总值比重由 21.6% 提升至 39.8%。

新型基础设施建设提速，数字产业化深入推进。截至今年 5 月底，我国已建成全球规模最大、技术领先的网络基础设施，所有地级市全面建成光网城市，千兆用户数突破 5000 万，5G 基站数达到 170 万个，5G 移动电话用户数超过 4.2 亿户。大数据、云计算、人工智能加速融入工业、能源、医疗、交通、教育、农业等行业。截至今年 6 月底，工业互联网应用已覆盖 45 个国民经济大类，工业互联网高质量外网覆盖 300 多个城市。

<https://mp.weixin.qq.com/s/v3Dui6ib8sAcV7aP9pI4Kg>

4、IDC：2021-2026 年中国数字化转型市场预测

国际数据公司（IDC）于近日发布了《中国数字化转型市场预测，2021-2026：通过应用场景践行数字化优先策略》研究报告。报告核心观点如下：

未来五年是数字化发展的黄金时期。2022 年，无论全球

还是中国，超过 50% 的经济 (中国约超 60 万亿元人民币) 是基于数字化或受数字化影响的，中国 2022-2026 年数字化转型总支出将达到 2.38 万亿美元。

中国数字化转型支出硬件主导，但软件和云部署模式支出增长更快。中国数字化转型支出中硬件目前仍然占比最大，未来 5 年将一直保持 48.6% 左右的市场份额。软件增长最高，2021-2026 年复合增长率 CAGR 达到 24.5%。在部署模式上，云部署相关的数字化转型支出在 2021 年占比为 12.8%，2021-2026 年复合增长率 CAGR 达到 31.5%，高于中国整体云市场 26.3% 的增长率，2026 年占数字化转型支出的占比也将提升至 21.2%。

<http://www.199it.com/archives/1455255.html>

5、勒索软件数量在一个季度内几乎翻了 2021 年的总量

每当一个勒索软件团伙退出 (REvil 或 Conti)，就会有更多的步骤来填补空白 (Black Basta)。

在 2021 年被勒索软件困扰之后，攻击量在 2022 年继续激增。上周二 WatchGuard 威胁实验室发布的一份报告显示，今年前三个月的勒索软件检测量是 2021 年同期的三倍。同时，2022 年第一季度的勒索软件数量相当于 2021 年全年记录的总量的 80% 以上。

尽管一个主要的勒索软件组织在 2021 年底倒台（REvil），但统计数字仍然越来越高，这证明了犯罪分子坚持改革、重塑和重组犯罪团伙，以从勒索软件策略中获利丰厚。

https://www.darkreading.com/attacks-breaches/ransomware-volume-doubles-2021-totals-single-quarter?&web_view=true

业界观点

1、解读与建议：关于开展数据安全认证工作的公告

6月9日，国家市场监督管理总局和国家互联网信息办公室联合发布了“关于开展数据安全认证工作的公告”（文号为2022年第18号，以下简称18号文）。

18号文的发布，第一次表明了国家主管部门将加强对数据安全的规范化管理，开展统一的认证工作，并发布《数据安全认证实施规则》，以明确对网络运营者开展网络数据收集、存储、使用、加工、传输、提供、公开等处理活动进行认证的基本原则和要求。

18号文明确要求参照国家标准《GB/T 41479-2022 信息安全技术 网络数据处理安全要求》的数据安全管理认证（DSM），这是对基于国内标准数据安全认证的重要补充与完善。

《数据安全认证实施规则》要求针对网络运营者的数据安全管理体系开展认证活动，因此建议组织的数据安全管理体系建设应在《网络数据处理安全要求》的基础上，从以下五个方面开展组织数据安全管理体系建设，以满足数据安全合规和保护组织数据安全的要求。

（一）数据安全规划。从数据安全总体策略、数据处理

的业务影响分析和风险评估、数据的分类分级、数据保护目录和数据保护计划五个方面进行数据安全规划。

（二）数据安全治理机制。从数据安全组织与职责、数据安全制度与流程、数据安全评估与考核、数据安全教育与培训四个方面来建立数据安全治理机制。

（三）数据安全生命周期管理。参考《网络数据处理安全要求》的相关内容。

（四）数据安全技术应用。数据安全建设不是单一的产品或工具的构建，而是覆盖数据全生命周期、结合组织自身使用场景的体系建设。应依据组织数据安全建设的方针策略，围绕数据全生命周期各阶段的安全要求，建立与制度流程相配套的技术和工具。

（五）数据安全运营。数据安全管理和技术体系的落地，离不开数据安全运营。首先应当把数据安全纳入组织的网络安全体系中，然后可从数据处理风险监测、数据安全事件管理、数据安全应急管理、数据安全审计等方面来建设运营体系。

<https://www.secrss.com/articles/44126>

2、杜跃进：数字安全进入能力主义时代

“加强数字安全保障不仅是因为政策要求,还因为企业确

实需要规避被网络攻击的风险,减少本可以避免的损失,这是企业的刚需。”近日,三六零(下称“360”)首席安全官杜跃进在世界智能大会上发表了题为“数字安全进入能力主义时代”的演讲。

杜跃进表示,数字安全的本质是人和人的对抗,它并不能够简单地用自然科学领域的规律来解决问题,不存在某种单一的技术彻底解决安全问题,因此企业需要从过去的安全产品为中心的思路转向以数字安全能力为中心的体系化思路上来。

如何应对数字安全风险?杜跃进认为,合规只是一个基本要求 and 底线,依靠堆积安全产品的方法,已经不能帮助企业有效应对网络安全威胁。目前,对于数字安全而言,能力成熟度是安全治理的重要抓手。

近两年大量和安全相关的标准开始聚焦能力或者能力成熟度,国内外安全战略政策开始重视和加快推进安全能力或能力成熟度相关的内容。“没有安全底座,就没有健康发展,数字安全事关数字革命的成败。”杜跃进表示,对于正在数字化转型的各行各业来说,当前最重要的任务就是提升数字安全能力,这是一切数字化工作正常进行的前提。而未来的安全,将是基于数据、依靠协同的安全能力体系,并在实际运营中持续进化,如此才能更好地护航企业数字化转型,整体性提升数

字安全水平。

https://wxh.xzdw.gov.cn/wlaq/aqdt/202206/t20220629_257878.html

3、沈浩：大数据视域下的数据伦理与消费者保护

针对数据使用对不同群体的影响的研究表明，数据伦理问题涉及更广泛的主题及非常实际的社会问题，通过践行数据伦理有助于减轻无意中融入系统、政策和服务的负面影响和偏见，从而创造更公平的社会。

大数据伦理下消费者保护面临的问题主要包括：消费者进行相关活动时产生的数据归属问题有待明确；相关消费数据缺乏透明性，虚假数据泛滥；相关法律法规有待完善，消费者疲于维权；大数据算法效用的双面性带来的问题。

因此，在加强数据伦理与消费者保护方面提出如下建议：推进消费者保护的立法工作落地，促使消费者权益保护有章可循、有法可依；强化数据伦理及消费者保护的多维度监督，构建并健全可落地的消费者保护监管体系；普及大数据隐私保护教育，增强消费者保护和数据伦理意识；推动大数据主体机构完善敏感数据的全周期保护制度。

https://www.sohu.com/a/561391962_603349

4、刘典：构建数据基础制度安全网

构建数据基础制度，将进一步推动我国数字经济治理体系和治理能力现代化，为培育壮大数据要素市场提供有力制度保障。建立起符合发展规律、适应发展趋势的数字基础制度，形成制度框架下的数据行为范式，有助于促进数据要素健康有序流动。同时，这还事关我国数字经济发展顶层设计和体制机制建设，有利于数据充分发挥要素作用，健全数据市场规则，降低交易成本，激发社会创新活力。

进一步提升数据基础制度的安全系数，须加强各方统筹协调，多措并举。

一是要以安全促发展，筑牢数据基础制度发展的安全保障。应把安全贯穿于数据开发的全过程。企业要坚持系统性、持续性的数据安全治理，覆盖数据、业务、技术、管理等多个方面。政府及相关部门应将数据安全治理贯穿立法执法司法全过程，激活数据市场的活力与张力。应构建政府、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。应打通技术与治理的双重通路，为数据安全保护提供技术支持及法律、政策保障。

二是要以发展促安全，进一步增强安全防护能力。一是探索合理有效的数据要素产权、交易、分配制度，充分发挥数据生产要素作用，推动经济增长；二是依靠数字经济发展

带动网络安全产业增长，加强数据保护和监管的技术能力建设及研发投入；三是加强数字技术人才培养和使用，增强全民数字素养，提升国家网络和数据安全防护能力。

三是要探索监管与市场服务相结合的安全治理体系。应建立安全可控、弹性包容的数据要素安全治理制度，为数字经济夯实前行道路。

<http://news.cnfol.com/guandianpinglun/20220630/29711150.shtml>

5、知网突遭审查，孔德亮：数据安全关乎国家安全，合规是生命线

为防范国家数据安全风险，维护国家安全，保障公共利益，依据《国家安全法》《网络安全法》《数据安全法》，按照《网络安全审查办法》，2022年6月23日，网络安全审查办公室约谈同方知网(北京)技术有限公司负责人，宣布对知网启动网络安全审查。

奇安信集团副总裁、创新BG负责人孔德亮表示，随着《数据安全法》的落地，国家相关部门对掌握重要数据企业的网络安全审查力度将显著加大，此次知网被安全审查，带来了以下几方面的启示：

首先是本次审查，再次表明数据安全已上升到国家安全

的高度。

其次，近年来高校、科研院所等拥有我国前沿学术研究成果的机构，其核心数据已经成为重点攻击目标。

第三，对于掌握重要敏感数据的企业机构，尤其需要将数据安全作为生命线，确保安全合规、不踩红线。

<http://www.itbear.com.cn/html/2022-06/433200.html>

数据安全事件

1、RansomHouse 团伙声称从芯片制造商巨头 AMD 窃取了 450GB 数据

2022 年 6 月 29 日报道，RansomHouse 勒索团伙声称在 2021 年从芯片制造商巨头 AMD 那里窃取了 450 GB 的数据，并威胁说如果该公司不支付赎金，就会泄露或出售这些数据。

<https://securityaffairs.co/wordpress/132721/cyber-crime/ransomhouse-hacked-amd.html>

2、密苏里州菲茨吉本医院遭勒索软件攻击，敏感数据泄露

2022 年 6 月 27 日，据外媒报道，密苏里州菲茨吉本医院遭到“Daixin Team”勒索团队袭击，其声称已经泄露了 40 GB 的数据，并提供了文件列表。

在浏览了完整的漏洞后，研究人员发现了许多包含受保护的患者健康信息的文件——在不同的文件和字段中，包含患者姓名、诊断或治疗信息、服务日期、健康保险信息和账单数据等等。同时，还发现了一个文件夹，其中包含从 2020 年至今的数千个关于癌症患者的扫描 pdf 文件，并附有详细的医疗报告。除了有关患者的信息外，还有与指定员工有关

的文件。

https://www.databreaches.net/mo-fitzgibbon-hospital-hit-by-ransomware-sensitive-data-leaked/?web_view=true

3、沃尔玛拒绝承认遭 Yanluowan 勒索软件攻击

2022 年 7 月 1 日，据外媒报道，虽然黑客声称成功入侵并对数千台计算机进行了加密，但是美国零售商沃尔玛否认遭到 Yanluowang 团伙的勒索软件攻击。沃尔玛在给 BleepingComputer 的一份声明中表示，他们的“信息安全团队正在 24/7 全天候监控系统”，并认为这些说法不准确。

勒索软件团伙声称在一个多月前进行了攻击，并且能够加密设备但没有窃取任何数据。作为这次攻击的一部分，他们说他们要求支付 5500 万美元的赎金，但从未收到沃尔玛的回应。

数据泄漏站点上的条目包括各种文件，这些文件声称包含在攻击期间从沃尔玛的 Windows 域中提取的信息。虽然沃尔玛否认攻击成功，但这些文件包含声称来自沃尔玛内部网络的信息，包括安全证书、域用户列表以及 kerberoasting 攻击的输出。

<https://www.cnbeta.com/articles/tech/1287509.htm>

4、Carnival Cruises 因数据泄露事件被罚款 125 万美元

2022 年 6 月 27 日称，Carnival Cruises 因 2019 年的数据泄露事件被罚款 125 万美元。该事件于 2019 年 5 月被发现，在 10 个月后的 2020 年 3 月才被披露，泄露了 180000 个员工和客户的信息，涉及姓名、社会安全号码、地址、护照号码、驾驶执照号码、支付卡信息和健康信息等。司法部长指出，该公司将个人信息存储在电子邮件中，并使用杂乱无章的方法来处理敏感数据，使违规通知变得更加困难。除了经济处罚外，该公司还同意实施违规响应计划，为员工制定邮件培训计划，接受独立的信息安全评估等。

<https://therecord.media/carnival-cruises-to-pay-1-25-million-fine-for-2019-data-breach/>

5、工行收集与业务无关的消费者金融信息等，被罚 618.7 万元

6 月初，工商银行安徽省分行因存在未按规定开展持续客户身份识别、未按规定重新识别客户、未按规定对高风险客户采取强化识别措施、部分 ETC 预登记业务办理未经消费者明示同意、漏报投诉数据等多项主要违法行为被警告并处罚款 618.7 万元。

<https://mp.weixin.qq.com/s/Kn4p3WWmcBrNSVswpbuYYg>

6、Cyble 称有超过 90 万个配置错误的 Kubernetes 暴露在网上

2022 年 6 月 29 日报道，Cyble 的一项分析发现，有超过 900000 个 Kubernetes 暴露在网上。Kubernetes 是一个高度通用的开源容器编排系统，如果配置不正确，可被远程攻击者访问内部资源和私有资产。研究人员使用与攻击者类似的扫描工具和搜索查询来定位暴露的 Kubernetes 实例，发现其中 65%（585000 台）位于美国，9%位于德国，而荷兰和爱尔兰各占 6%；暴露最多的 TCP 端口是 443，其次是端口 10250 和 6443。。

<https://www.infosecurity-magazine.com/news/misconfigured-kubernetes-exposed/>

7、加利福尼亚州的枪支管制网站暴露个人数据

2022 年 6 月 30 日，据外媒报道，加利福尼亚州的一个网站披露了 2011 年至 2021 年期间申请隐蔽携带武器 (CCW) 许可证的所有用户的个人详细信息。

根据加州司法部的说法，该事件发生在本周早些时候，当时美国各州的枪支门户网站正在进行检修。除了该门户网站之外，该州提供的其他几个在线 dashboard 也发生了数据泄露，包括：突击武器登记处、经认证出售的手枪、经销商

销售记录、枪支安全证书和枪支暴力禁制令仪表盘。

卡利司法部指出，仪表板和数据对公众开放“不到 24 小时”，公开的信息包括姓名、出生日期、性别、种族、驾驶执照号码、地址和犯罪记录，一些私人信息可能已经发布在社交媒体网站上。

https://www.theregister.com/2022/06/30/california_websites_expose_personal_data/?&web_view=true

8、OpenSea 披露数据泄露，警告用户网络钓鱼攻击

2022 年 6 月 30 日报道，最大的非同质化代币 (NFT) 市场 OpenSea 29 日披露了一起数据泄露事件，并警告用户注意未来几天可能针对他们的网络钓鱼攻击。

在线 NFT 市场表示，它拥有超过 60 万用户，交易量超过 200 亿美元。该平台的电子邮件递送供应商 Customer.io 的一名员工下载了属于 OpenSea 用户和时事通讯订阅者的电子邮件地址。由于事件中被盗的电子邮件地址也与未经授权的外部方共享，因此 Hardman 敦促可能受影响的用户对冒充 OpenSea 的网络钓鱼尝试保持警惕。

https://www.bleepingcomputer.com/news/security/opensea-discloses-data-breach-warns-users-of-phishing-attacks/?&web_view=true