全球数据安全观察

总第 116 期 2022 年第 44 期

(2022.11.28-2022.12.04)

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、《上海市浦东新区促进无驾驶人智能网联汽车创新应用规定》发布.....1
2、《贵州省信息基础设施条例》发布.....1
3、国内首个数据知识产权登记系统正式上线.....2
4、国家标准《工业互联网企业网络安全 第 4 部分：数据防护要求》公开征求意见.....2
5、SDK 个人信息处理规范等 9 项电信团体标准发布.....3
技术、产品与市场.....5
1、Gartner 发布 2022 年中国安全技术成熟度曲线.....5
2、IDC 发布《2021 年中国数字政府 IT 解决方案市场份额》.....6
3、欧盟公布量子技术 2030 年路线图，抢占未来十年.....7
4、2022 年暗网市场三大趋势.....7
5、研究：金融机构更容易发生意外数据泄露.....9
业界观点.....10
1、魏亮：三重体系下，数据流通安全的挑战与对策.....10
2、晓超：进一步加强数据制度体系顶层制度设计.....11
3、数据要素市场培育应以安全为基石.....13
4、织密金融数据安全防护网.....14

5、中国数据开放共享如何向纵深迈进？ 15
数据安全事件 18
1、因泄露 5.33 亿用户隐私，Facebook 被罚 2.65 亿欧元 .. 18
2、法国电力供应商因使用弱 MD5 算法存储用户密码被罚款 18
3、Sony、Lexar 等闪存设备加密提供商泄露敏感数据一年有余 19
4、密码神器 LastPass 承认黑客窃取了客户数据 19
5、哥伦比亚医疗机构 Keralty 遭到 RansomHouse 的勒索攻击 20
6、医疗软件商 Connexin Software 陷危机，119 家儿科诊所 220 万患者信息被泄露 20
7、俄罗斯政府机构遭 CryWiper 勒索软件攻击 21
8、宜家商场数据被勒索团伙发布至网站 21
9、勒索软件集团从英国自来水公司窃取了客户的银行详细信息 22
10、Anker 未经用户同意向云端上传信息 23

政策形势

1、《上海市浦东新区促进无驾驶人智能网联汽车创新应用规定》发布

11 月 23 日，上海市第十五届人民代表大会常务委员会第四十六次会议通过《上海市浦东新区促进无驾驶人智能网联汽车创新应用规定》，自 2023 年 2 月 1 日起施行。

条例明确规定开展智能网联汽车创新应用的企业应当按照有关规定，**严格保护高精度地图数据安全**，建立健全**全流程数据安全和个人信息保护管理制度**，落实**数据安全和个人信息保护责任**。

https://www.shrd.gov.cn/n8347/n8467/u1ai250242.html

2、《贵州省信息基础设施条例》发布

12 月 1 日，《贵州省信息基础设施条例》经贵州省第十三届人民代表大会常务委员会第三十六次会议修订通过，自 2023 年 3 月 1 日起施行。

条例强调信息基础设施运营者应当**加强网络和数据安全保护**，落实网络安全等级保护要求，建立健全监测预警、风险评估体系和责任认定制度，制定完善应急预案，定期开展应急演练，积极处置网络安全事件，按照规定及时告知用

户并向网信、公安机关、通信、大数据等有关部门报告。

http://www.echinagov.com/policy/333176.htm

3、国内首个数据知识产权登记系统正式上线

日前，在深圳市市场监督管理局（深圳市知识产权局）的指导下，由深圳市标准技术研究院自主开发建设的“数据知识产权登记系统”（https://sjdj.sist.org.cn/）正式上线。

该系统为经过一定规则处理的、具有商业价值的非公开数据提供数据知识产权登记服务，向提出登记申请的数据处理者颁发数据知识产权登记证书。

http://www.szar.org.cn/news/2508

4、国家标准《工业互联网企业网络安全 第4部分：数据防护要求》公开征求意见

12月1日，全国通信标准化技术委员会、全国信息安全标准化技术委员会双归口的国家标准《工业互联网企业网络安全 第4部分：数据防护要求》公布标准征求意见稿面向社会征求意见，该意见稿规定了不同级别工业互联网数据的安全防护流程、防护要求和安全管理要求。

https://www.secrss.com/articles/49616

5、SDK 个人信息处理规范等 9 项电信团体标准发布

11 月 25 日，电信终端产业协会（TAF）公开发布 9 项电信领域团体标准。

其中，《APP 收集使用个人信息最小必要评估规范 第 1 部分：总则》明确 APP 收集使用个人信息最小必要评估规范系列标准中术语定义，规定了收集使用的最小必要原则及要求。

《软件开发包（SDK）个人信息处理规范》规定了对外提供服务的软件开发包（SDK）个人信息处理规范，包括软件开发包（SDK）处理个人信息的基本要求、软件开发包（SDK）提供者的基本要求以及保障及时响应用户权利的要求。

《基于差分隐私的用户个人信息保护技术要求》规范了基于差分隐私的用户个人信息保护技术要求，包括差分隐私系统技术架构、差分隐私能力要求、差分隐私保护分级、差分隐私保护效果评定。

《App 推荐算法用户权益保护技术要求及测评规范》规定了 App 推荐算法在用户权益保护方面应满足的基本原则、个人信息保护要求、推荐算法技术安全要求、用户主体权益保护要求、推荐算法安全管理要求及测评方法。

《电信和互联网个人信息保护能力审计规范》规定了个

人信息保护合规审计规范，主要包括审计目标、审计原则、审计范围、审计管理、审计内容、审计工具功能和审计评估。

https://mp.weixin.qq.com/s/b4SQldNkHaknjGlVdXkWXg

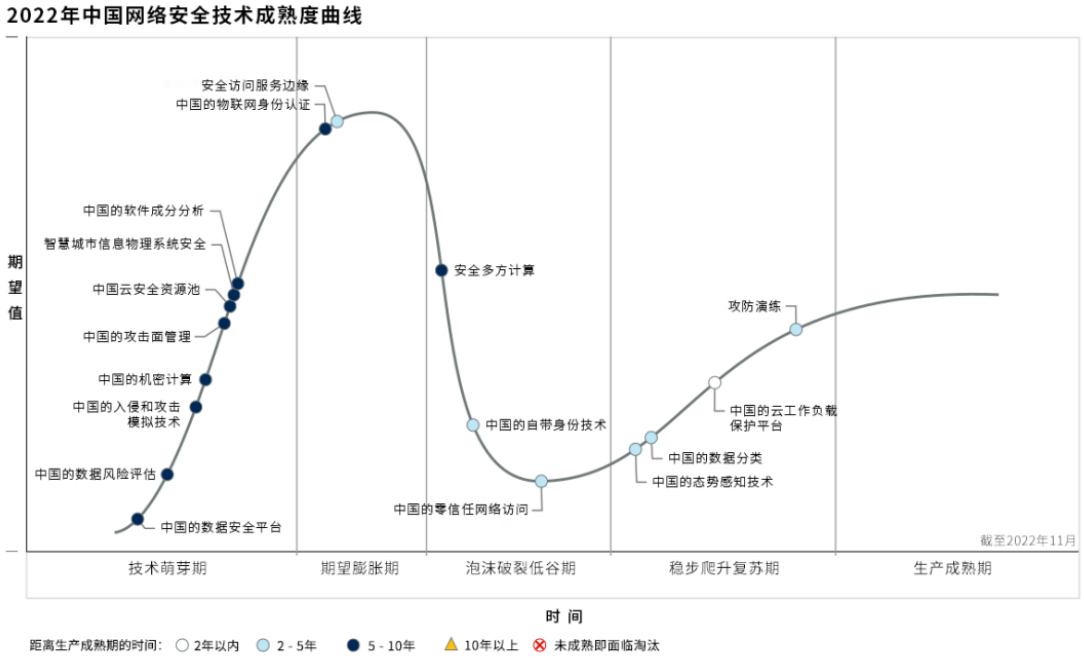
技术、产品与市场

1、Gartner 发布 2022 年中国安全技术成熟度曲线

Gartner 于 2022 年首次发布《2022 年中国安全技术成熟度曲线》，该曲线指出，随着国内数字化转型的推进，尤其是云计算、大数据、人工智能、物联网和电子商务的发展，企业机构数字资产保护已成为安全和风险管理领导者的关键任务。

国内法规日趋严格，安全的重要性更甚以往。这篇报告是全新的中国安全创新领域技术成熟度曲线。中国安全技术与市场，在技术成熟度、产品、供应商等方面与国际市场存在差异，因此针对国内特点筛选了一批创新安全技术和服务。

报告中，萌芽阶段包括数据安全平台、数据风险评估、入侵与攻击模拟、机密计算、攻击面管理、云安全资源池、智慧城市网络物理系统安全、软件组成分析技术；**膨胀阶段**包括物联网认证、安全访问服务边缘；**破裂阶段**包括安全多方计算、自备身份、零信任网络访问技术；**爬升阶段**包括态感知、数据分类、云工作负载保护平台、攻防演练。



https://www.secrss.com/articles/47892

2、IDC 发布《2021 年中国数字政府 IT 解决方案市场份额》

IDC 于近日发布了《中国数字政府 IT 解决方案市场份额，2021》报告，聚焦于数字政府的行业应用 IT 解决方案市场，介绍了行业内的核心解决方案提供商，并着重选取法院与检察院、财政、税务、人力资源与社会保障、市场监管、自然资源等垂直子行业进行分析，提供了市场发展趋势与子市场的厂商市场份额。

2021 年数字政府 IT 解决方案市场规模为 275.8 亿元人民币，同比增长 32.3%。回顾 2021 年中国数字政府应用 IT 建设情况，IDC 发现以下几个特征：

（1）信息系统协同化，系统间更紧密的对接与数据互通。

（2）政务数据集中化，云化与智慧化趋势明显。

（3）项目建设运营化，建设与运营模式变革中。

https://www.secrss.com/articles/49545

3、欧盟公布量子技术 2030 年路线图，抢占未来十年

欧盟量子技术战略将全面更新，量子旗舰计划(Quantum Flagship)刚刚发布了初步的战略研究和产业议程(SRIA)，提出了一条与欧盟各种量子技术倡议相一致的实施路径，预计将于 2023 年发布的最终 SRIA 中会有更全面的战略更新。

作为核心，这份初步 SRIA 文件概述了四大技术支柱**量子计算、量子模拟、量子通信、量子传感和计量**以及劳动力发展和标准化等横向问题的 2030 年路线图。

https://www.secrss.com/articles/49628

4、2022 年暗网市场三大趋势

据《网络犯罪》预测，2023 年全球网络犯罪造成的损失将高达 8 万亿美元，网络犯罪市场将成为规模仅次于中国和美国的全球第三大“经济体”，其“GDP”增速更是高达 15%。暗网市场的繁荣得益于（导致数据泄露的）网络攻击的快速增长。根据网络安全公司 SonicWall 最新公布的数据，2022

年网络攻击全面增长，各种技术和策略不断丰富，从入侵和恶意软件到较新的攻击媒介，如加密劫持和 NFT 犯罪。

以下是 2022 年值得关注的暗网市场三大新趋势:

（1）暗网市场爆发“价格战”。 2022 年暗网产品价格普遍下降，从恶意软件和拒绝服务攻击到加密货币交易所的失窃账户都不能幸免。

（2）六大热门暗网市场。2022 年规模最大的六个暗网市场（按市场份额百分比排序）:

- Dark0de：37%
- ToRReZ：30%
- DarkFox：21%
- ASAP：10%
- Cannazon：2%
- G.Dreams：不到 1%

（3）240 亿用户账户“上市流通”。 根据 DigitalShadows 发布的数据泄露报告“2022 年账户接管调查”，2022 年总计超过 240 亿用户账户凭证在暗网论坛和犯罪市场中流通，这个数字比两年前暴增了 65%。

https://www.secrss.com/articles/48824

5、研究：金融机构更容易发生意外数据泄露

Netwrix 公布了其全球 2022 年云安全报告中针对金融和银行业的调查结果。与接受调查的其他行业相比，金融机构更关心能够合法访问其云基础设施的用户。

事实上，该行业 44% 的受访者表示，他们自己的内部 IT 员工对云中的数据安全构成了最大风险，47% 的人担心承包商和合作伙伴，而在接受调查的其他垂直行业中，这一比例分别只有 30% 和 36%。

“与其他垂直行业的公司相比，金融机构更容易遭遇意外数据泄露: 32% 的金融机构在过去 12 个月内报告了此类安全事件，而平均水平只有 25%。为了应对这一威胁，组织需要实施一种零特权方法，在这种方法中，只有在需要时才授予提升的访问权限，并且只在需要的时候授予，” Netwrix 安全研究副总裁 Dirk Schrader 评论道。

“云配置错误是意外数据泄露的另一个常见原因。因此，安全团队必须持续监控其云配置的完整性，最好是使用自动化流程的专用解决方案。”

https://www.helpnetsecurity.com/2022/12/02/financial-sector-cloud-security/?web_view=true

业界观点

1、魏亮：三重体系下，数据流通安全的挑战与对策

近日，在2022中国互联网大会数据安全论坛上，中国信息通信研究院副院长魏亮介绍了数据流通包括的流通数据、流通活动、流通设施三个层次，他认为在数据流通的过程中，数据安全的内涵也不断拓展，数据安全保护的对象也从传统的数据安全拓展到三个层次：数据本身的安全，数据流通活动的安全，数据流通设施的安全。

针对以上数据流通的三个层次，魏亮指明我国数据流通安全依旧面临以下挑战。

在流通数据层面：参与流通的数据形态日益丰富，数据资产梳理和分类分级难度加大。

在流通活动层面，数据资源高度集中，日趋复杂的新技术、新应用、新场景引发数据滥用、数据污染等问题。

在流通设施层面，数据流通设施平台开放互动增强，数据安全防护压力加大。

魏亮表示，围绕以上提到的数据流通三个层次的安全保障需要，应充分发挥政府、行业、企业各方资源和技术优势，推动形成多方协同、齐抓共管的治理格局。

政府部门应通过政策引领等方式，在流通数据层，明确

各类各级数据差异化的流通条件和安全要求，并结合流通利用和安全保护需求制定流通数据负面清单；在流通活动层，探索分级分层市场准入、“沙盒”监管等创新机制，适度给予创新容错空间；在流通设施层，建立交易平台准入评估机制，探索建设跨区域一体化数据流通平台、“数据银行”等基础设施，搭建安全流通环境。

行业机构应结合各领域特点，在流通数据层，加快制定数据分类分级标准规范，开展非结构化数据、重要数据自动识别、分析、达标等技术攻关；在流通活动层，开展安全多方计算、联邦计算、数据水印等流通安全技术攻关；在流通设施层，大力发展面向流通需求的安全检测、评估、认证等专业服务。

企业主体应全面落实国家和行业数据分类分级管理要求，在流通数据层，积极应对新技术提升数据分类分级的及时性和准确度；在流通活动层，建设内部数据流通安全一体化管理平台，强化政企协同联动；在流通设施层，定期开展流通设施安全监测评估，持续提升安全保护能力。

http://iitime.com.cn/html/10201/745369.htm

2、晓超：进一步加强数据制度体系顶层制度设计

晓超表示，相比于数据规模的迅猛扩张和应用场景的不

断创新，我国数据制度体系仍然存在短板，须进一步加强顶层制度设计，从数据产权、流通交易、收益分配、安全治理等方面入手构建数据基础制度体系，促进数据高效流通使用。

因此，**要加快建立数据要素产权制度**。尽快分类分级推进公共数据、企业数据、个人数据确权授权使用，建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制，健全数据要素权益保护制度等，使数据确权更精准，数据流动更通畅。

要加快建立数据要素流通和交易制度。完善数据全流程合规和监管规则体系，建设规范的数据交易市场，激励更多主体参与数据要素市场。做好数据流通交易这篇大文章，建立规范、科学、安全的市场规则，将进一步促进数据资源高效配置。

还**要加快完善数据安全治理制度**，破解制约数据要素市场化的难题。应建立健全数据安全治理体系，提高数据安全保障能力。维护国家数据安全，保护个人信息和商业秘密，把安全贯穿数据治理全过程。压实企业数据安全责任，促进政府、企业等携手筑牢数字安全屏障。

http://www.china-cer.com.cn/shuzijingji/2022112822339.html

3、数据要素市场培育应以安全为基石

近年来，随着《网络安全法》《数据安全法》《个人信息保护法》等一系列基础性法律法规落地实施，我国已建立起一套基本的网络安全法律合规框架，国家开展数据安全治理制度依据逐渐完善。

“积极贯彻落实法律法规要求，数据安全机制正呈现协同化、全面化、精细化、多元化的发展趋势。”中国移动集团信息技术中心副总经理黄岩在谈到国内数据安全工作时说到，“如今，各地区、各有关部门各司其职，评估、认证、检查等多种工作方式综合治理，多种工作机制相互补充，有效推进了数据安全的治理工作。”

除了在法律上积极引导数据流通安全，使数据安全相关工作有法可依外，数据安全举报投诉机制也在不断完善，以充分发挥公众监督作用。今年年初，中国互联网协会制定发布了电信和互联网行业数据安全举报投诉处理工作规则，依托 12321 网络不良与垃圾信息举报受理中心，受理关于数据安全的举报投诉。

“对于数据安全举报投诉机制，一是加强数据安全管理；二是保障数据安全；三是保护个人组织的合法权益；四是维护国家安全和发展利益。”中国互联网协会监管支撑部主任郝智超发言称。

“数据安全和个人隐私保护是持续的常态化过程，需要包括监管、研究机构、学术机构、产业界等不同携手合作，打造良好的安全生态环境，持续开展数据安全治理研究实践，才能共同守护数字经济健康发展。”蚂蚁集团数据安全总经理郭亮说道。

https://www.handannews.com.cn/news/content/2022-11/29/content_20058338.html

4、织密金融数据安全防护网

当前，金融数据面临多重问题和挑战，特别是在不同业务间、机构间流转的过程中，从技术到管理都面临众多潜在的安全风险，需要加强安全设置和制度保障。

强化数据安全治理，巩固金融安全阵线。当下，由于数字技术促使数据应用场景和参与主体日益多样化，数据安全的外延不断扩展，数据安全治理亟待完善。金融数据是数字金融的基础，加强相关数据安全治理的重要性不言而喻。要完善数据安全管理体系，包括建立数据分级分类管理制度，落实技术和管理措施等。应对数据安全各方面问题能够及时识别，分析出所识别的数据安全问题源头。要形成常态化的控制机制和技术手段，形成应急机制，把安全问题控制在最小范围内。

筑牢金融安全网，以安全治理促高质量发展。国家“十四五”规划将网络安全确定为未来中国发展建设工作的重点之一。《“十四五”数字经济发展规划》提出着力强化数字经济安全体系，从国家顶层设计层面强化网络安全的重要地位。只有先行构筑牢固的金融安全网，才能避免重大风险，为数字金融提供高质量发展环境。应构建金融主体高管层、安全专业部门等共同参与的治理体系，开展数据安全等级标签化和线上化管理，利用自然语言处理技术，实现敏感信息的自动识别与安全分级。在监管模式方面，要加快探索适合于中国数字金融发展的新监管模式，使数字金融能够纳入到整个金融监管中去，同时提高监管的数字化、智能化水平。

http://www.cbdio.com/BigData/2022-12/02/content_6171228.htm

5、中国数据开放共享如何向纵深迈进？

数据开放共享是各国推进数字经济发展过程中都无法回避的核心问题。欧美等发达国家因起步较早，已逐渐形成了一些较为成熟的数据开放共享经验。包括：制定政策执行机制，确保数据开放落到实处；确立统一的数据基础设施和规范标准，提高数据质量，扫除数据共享过程中遇到的标准障碍；支持政府与各界建立合作关系，创新数据使用，促进

数据商业化。

汲取欧美的数据开放共享经验，结合我国国情，我国可从以下四个方面提升数据开放共享水平:

完善数据开放机制。制定数据开放政策落实机制，确保相关政策落到实处；制定并发布统一、权威的公共数据开放目录，探索建立数据开放许可协议机制，明确数据开放各方权责，提升数据开放质量，规范数据开发利用；出台数据分级分类的政策法规，明确可开放数据的范围，推进数据去标识化技术应用，完善各敏感程度数据的开放管理规定，化解制约公共数据开放所面临的个人隐私、商业秘密、国家安全等潜在风险。

支持政企合作，促进数据商业化。建立更为健全的政府、企业互动交流机制，积极开展企业对公共数据的需求调研，在确保安全的前提下，以数据分类分级为基础，精准对接企业数据需求。根据相关需求明确数据开放的重点领域，提高数据开放的针对性，并针对需求较大的数据适当缩短更新周期，提升相关数据的及时性，从而促进数据创新，释放数据价值。

优化数据开放平台。构建出全国统一的公共数据开放平台体系，逐步形成一站式、便捷化、全口径的公共数据开放服务能力。在平台功能方面，不断强大搜索功能，加强完善

二级搜索，增强对数据的分级分类管理、关联数据管理，便捷社会公众；加强互动和交流板块的设计，及时展示意见交流和互动情况。在数据保护方面，应建立健全公共数据开放平台的安全管理机制，加强密码技术、身份鉴别技术、数据沙箱技术等关键技术的研究和应用，防范和化解公共数据汇聚、开放可能引发的各类数据安全风险挑战。

加强数据安全保护。逐步建立起更加完善的细分领域的数据安全法律法规，形成数据防泄露、安全审计、安全事件溯源与取证、大数据安全态势分析等运维管理制度。同时，解决数据安全保护问题，需要构建起有效的数据安全解决方案，利用数据交换监控技术、数据加密脱密技术、敏感信息匿名化等技术，创建起受隐私保护与安全防护约束的新型计算范式，实现数据在开放共享过程中的安全防护。

https://mp.weixin.qq.com/s/0-wx100M4-O4w3uIpXmBoQ

数据安全事件

1、因泄露 5.33 亿用户隐私，Facebook 被罚 2.65 亿欧元

11 月 28 日消息，爱尔兰数据保护委员会 (DPC) 因 2021 年 Facebook 大规模数据泄露事件，向其母公司 Meta 开出 2.65 亿欧元（约 20 亿人民币）巨额罚单。DPC 辩称 Meta 违反了 GDPR，因为它没有实施适当的技术和组织措施，也没有按照欧洲法规的要求采取必要的保障措施，违反了 GDPR 第 25(1)和 25(2)条。

https://www.bleepingcomputer.com/news/security/meta-fined-265m-for-not-protecting-facebook-users-data-from-scrapers/

2、法国电力供应商因使用弱 MD5 算法存储用户密码被罚款

据媒体 11 月 30 日报道，电力供应商法国电力公司(EDF)因违反欧盟通用数据保护条例(GDPR)，被法国数据保护监管机构罚款 60 万欧元。国家信息和自由委员会(CNIL)表示，该公司在 2022 年 7 月使用 MD5 算法对 25800 多个帐户进行 hash 处理来存储密码。此外，与 2414254 个账户相关的密码仅经过 hash 处理而未加盐，使账户持有人面临潜在的网络威胁。该调查还指责 EDF 未能遵守 GDPR 数据保留政策，并提供了关于所收集数据来源的不准确信息。

https://thehackernews.com/2022/11/french-electricity-provider-fined-for.html

3、Sony、Lexar 等闪存设备加密提供商泄露敏感数据一年有余

11 月 30 日，Sony、Lexar 或 Sandisk 等 USB 设备的加密解决方案提供商—荷兰软件公司 ENC Security 被曝出泄露配置和证书文件长达一年多。该公司表示，第三方供应商的错误配置导致了该问题，并在接到通知后立即修复。泄漏服务器中的数据包括销售渠道的简单邮件传输协议 (SMTP) 凭据、单一支付平台的 Adyen 密钥、电子邮件营销公司的 Mailchimp API 密钥、许可支付 API 密钥、HMAC 消息身份验证代码以及存储在.pem 格式。

https://cybernews.com/security/encsecurity-leaked-sensitive-data/

4、密码神器 LastPass 承认黑客窃取了客户数据

11 月 30 日，密码管理工具 LastPass 首席执行官 Karim Toubba 公开承认，通过一个新的漏洞，黑客访问了 LastPass 的第三方云存储服务器，并获得了部分客户的关键信息。但具体有多少客户因此受到影响，以及黑客窃取了哪些敏感信

息暂时未公布。

https://www.secrss.com/articles/49626

5、哥伦比亚医疗机构 Keralty 遭到 RansomHouse 的勒索攻击

媒体 11 月 30 日称，哥伦比亚的一家医疗保健提供商 Keralty 遭到 RansomHouse 的勒索攻击。攻击发生在上周日，Keralty 及其子公司 EPS Sanitas 和 Colsanitas 的 IT 运营、医疗预约安排及网站都受到了影响。本周一，Keralty 表示他们遇到了技术问题但没有透露原因。该公司又在周二发表声明，确认中断是由网络攻击造成的。RansomHouse 表示对此次攻击负责，并称已窃取 3 TB 数据。

https://www.bleepingcomputer.com/news/security/keralty-ransomware-attack-impacts-colombias-health-care-system/

6、医疗软件商 Connexin Software 陷危机，119 家儿科诊所 220 万患者信息被泄露

11 月 30 日消息，医疗软件商 Connexin Software 近期通知其数据泄露事件影响了 200 万个患者。该公司是一家为儿科医疗团队提供电子病历和执业管理软件、计费服务和业务分析工具的供应商。8 月，Connexin 在内网检测到数据异常，

之后立即展开调查。9 月，确认未经授权的第三方能够访问用于数据转换和故障排除的一组离线病人数据。

目前，Connexin 重置了所有公司帐户的密码，将患者数据移至更安全的环境中，并通过 Kroll 为受影响患者提供一年的身份监控服务。

https://www.bleepingcomputer.com/news/security/russian-cybergangs-stole-over-50-million-passwords-this-year/

7、俄罗斯政府机构遭 CryWiper 勒索软件攻击

12 月 1 日，外媒报道称，俄罗斯市长的办公室和法院遭到了一种新的加密病毒的攻击。

该程序在计算机上对数据进行编码，要求支付赎金——超过 50 万卢布。但是，即使您将这笔金额转移给黑客，病毒也会将文件完全删除。卡巴斯基实验室的专家解释说，CryWiper 会破坏所有格式文件的内容，它的主要用途是数据库、档案、个人用户文档，但不会自动销毁文件，它会向命令和控制服务器发送请求，只有在获得许可后才会开始工作。

https://www.securitylab.ru/news/535064.php

8、宜家商场数据被勒索团伙发布至网站

11 月 30 日消息，勒索软件团伙 Vice Society 将从宜家

摩洛哥和宜家科威特窃取的数据发布至该团伙的网站。宜家摩洛哥公司证实，该公司在摩洛哥和科威特都遭受了网络攻击。

来自勒索软件团伙泄密网站的片段表明，威胁行为者掌握了机密业务数据。文件和文件夹名称表明敏感的员工数据（例如护照）可能已经泄露。

https://cybernews.com/news/ikea-posted-ransomware-gang/

9、勒索软件集团从英国自来水公司窃取了客户的银行详细信息

12 月 1 日报道，为英格兰超过 170 万人供水的南斯塔福德郡水务公司（South Staffs Water）表示，今年 8 月份的一次勒索软件攻击事件可能让网络犯罪分子窃取了客户的银行详细信息。

据调查，该事件导致未经授权访问该公司为部分客户持有的部分个人数据，受影响的详细信息包括与客户账户关联的姓名和地址，以及用于设置直接借记付款的银行详细信息（帐号和分类代码）。

“我们收到的有关南斯塔福德郡水资源数据泄露的信息非常令人担忧。当一家如此大规模的公司遭遇数据泄露时，这意味着大量个人数据可能面临被滥用的严重风险，”该公

司的法律总监表示道。

https://therecord.media/ransomware-group-may-have-stolen-customer-bank-details-from-british-water-company/?web_view=true

10、Anker 未经用户同意向云端上传信息

11 月 30 日报道，消费电子品牌 Anker 旗下的 Eufy 安全监控探头被发现会在未启用云服务的情况下将用户信息和人脸的缩略图上传到云端服务器。

安全顾问 Paul Moore 购买了一个 Eufy Doorbell Dual，发现在未启用云服务时用户信息的缩略图会被上传。他发布了一则视频，演示了拍摄自己脸部视频，相关信息被上传到云端。即使没有注册云服务，从 Eufy 应用中删除视频，缩略图仍然能从网站访问。Eufy 没有上传完整视频，只是上传了缩略图。对于 Moore 的询问，Eufy 回应承认向其 AWS 服务上传了缩略图，表示数据不会向外泄露，因为 URL 是受限的，时间也有限制，而且需要账号登陆。但 Moore 还发现未加密的 Eufy 探头内容可以在没有身份认证的情况下访问。

https://www.solidot.org/story?sid=73518

《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

http://www.nelab-bdst.org.cn/