全球数据安全观察

总第 110 期 2022 年第 38 期

（2022.10.17-2022.10.23）

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、二十大：推进国家安全体系和能力现代化，坚决维护国家安全和社会稳定

中国共产党第二十次全国代表大会于 10 月 16 日上午在人民大会堂开幕。习近平代表第十九届中央委员会向党的二十大作报告。

报告指出，我们要健全国家安全体系，完善高效权威的国家安全领导体制，完善国家安全法治体系、战略体系、政策体系、风险监测预警体系、国家应急管理体系，构建全域联动、立体高效的国家安全防护体系。增强维护国家安全能力，坚定维护国家政权安全、制度安全、意识形态安全，确保粮食、能源资源、重要产业链供应链安全，维护我国公民、法人在海外合法权益，筑牢国家安全人民防线。提高公共安全治理水平，坚持安全第一、预防为主，完善公共安全体系，提高防灾减灾救灾和急难险重突发公共事件处置保障能力，加强个人信息保护。

http://lsrm.hinews.cn/xinwen/show-17027.html

2、14 项网络安全国家标准获批发布

根据 2022 年 10 月 14 日国家市场监督管理总局、国家

标准化管理委员会发布的中华人民共和国国家标准公告（2022 年第 13 号），全国信息安全标准化技术委员会归口的 14 项国家标准正式发布，包括“信息安全技术 步态识别数据安全要求”、“信息安全技术 个人信息安全工程指南”、“信息安全技术 汽车数据处理安全要求”、“信息安全技术 即时通信服务数据安全要求”等多个数据安全相关标准。

https://www.tc260.org.cn/front/postDetail.html?id=20221017101959

3、《信息安全技术 智能手机预装应用程序基本安全要求（征求意见稿）》发布

10 月 9 日，全国信息安全标准化技术委员会归口的国家标准《信息安全技术 智能手机预装应用程序基本安全要求》现已形成标准征求意见稿，面向社会公开征求意见。

征求意见稿给出了智能手机预装应用程序的基本安全要求，包括可卸载要求、安全功能及保障要求、个人信息安全要求等安全技术要求，预装行为安全、第三方预装应用程序安全管理、预装应用程序安全信息公示、投诉举报等安全管理要求。该标准适用于智能手机生产企业的生产活动，也可为相关监管、第三方评估工作提供参考。

https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20221009

202120&norm_id=20220921103038&recode_id=48947

4、浙江省湖州市发布《执法司法信息采集及共享交换技术规范(征求意见稿)》

10 月 20 日，浙江省湖州市人民检察院等单位发布了《执法司法信息采集及共享交换技术规范（征求意见稿）》，对了执法司法信息的数据采集、数据处理和存储、数据传输、数据共享、数据交换和数据管理等方面的要求进行了规定，其中通过权限管理、安全管理两个维度提出对数据的管理要求。

https://bz.zjamr.zj.gov.cn/public/news/view/CONSULTATION/641ba985cb724304b52dd2c25402e605.html

5、江西省印发《江西省数字经济领域关键技术目录》

近日，江西省科学技术厅印发了《江西省数字经济领域关键技术目录》。其中提到数字经济内涵极其丰富，涵盖的技术领域十分庞杂。**数字关键技术包括隐私计算、区块链、人工智能、元宇宙等**，数字融合关键技术包括数据确权、数据交易、数据定价算法等。

技术目录结合隐私计算数据脱敏技术、差分隐私技术、同态加密技术、安全多方计算技术、联邦学习技术、可信计算环境、个人信息保护技术等数字技术前沿领域发展趋势，

立足产业、技术发展基础和重点方向，尽可能系统完整地梳理相关技术目录，希望能为数字经济领域技术攻关和创新应用提供借鉴和参考，助力数字经济高质量发展。

https://mp.weixin.qq.com/s/VWx8JhBAlVhim6f5UG68GA

技术、产品与市场

1、IDC：2022 上半年中国 IT 安全服务市场厂商整体收入约为 12.25 亿美元 涨幅 11%

IDC《2022 上半年中国 IT 安全服务市场跟踪报告》显示，2022 上半年中国 IT 安全服务市场厂商整体收入约为 12.25 亿美元（约合 79.4 亿元人民币），厂商收入规模较去年同期实现平稳增长，涨幅 11%。

IDC 定义下的网络安全服务市场分别由安全咨询服务、IT 安全教育与培训服务、托管安全服务、安全集成服务四个子市场构成。**市场的具体表现如下：**

认证培训和安全实训演练测试平台与服务市场，共同推动 IT 安全教育与培训市场上半年实现高速增长：上半年，IT 安全教育与培训市场增速最快，规模同比增长达到 33%。其中，疫情之下，众多安全从业者/学生选择通过考证来提升其技能水平，这使得认证培训市场在上半年快速发展。除此之外，安全实训演练测试平台与服务在国家政策、大型活动、竞赛、科研等需求的推动下也实现了超高速增长。目前，该市场已经成为了推动企业级培训市场增长的主要推动力。

托管安全服务市场增速不及预期：上半年托管安全服务市场规模同比增长 15.6%，增速不及往年。具体来说，目前

中国整体托管安全服务市场结构仍以驻场托管为主。然而，疫情对于驻场托管市场的冲击较大，使得整体市场规模增速不及预期。当然，疫情侧面推动了远程托管以及云托管市场的发展，规模增速较快。但由于远程托管和云托管的市场规模较小，客单价较低，并没有逆转上半年整体市场增速下滑的状态。

咨询服务和集成服务市场受外部因素影响增长缓慢：上半年咨询服务和集成服务市场规模较去年同期近乎持平，其增速趋缓的原因主要与疫情下项目少、验收慢、回款难等因素相关。待疫情向好，咨询服务和集成服务市场将快速恢复，实现增长。

https://mp.weixin.qq.com/s/Qn2EaWHx2YzMeGoJKT6yBQ

2、Gartner 发布 2023 年十大战略技术趋势

近日，Gartner 发布企业机构在 2023 年需要探索的十大战略技术趋势。**Gartner 2023 年战略技术趋势围绕优化、扩展和开拓这三大主题**，这些技术能够帮助企业机构优化韧性、运营或可信度、扩展垂直解决方案和产品交付并利用新的互动形式、更加快速的响应或机会进行开拓。***2023 年重要战略技术趋势包括：***

优化主题：数字免疫系统（Digital Immune System）、应

用可观测性（Applied Observability）、AI 信任、风险和安全管理（Trust, Risk and Security Management）;

扩展主题：行业云平台（Industry Cloud Platforms）、平台工程（Platform Engineering）、无线价值实现（Wireless Value Realization）;

开拓：元宇宙（Metaverse）、超级应用（Superapps）、自适应 AI（Adaptive AI）。

https://www.secrss.com/articles/48041

3、Google 发布安全操作系统 KataOS 并开源参考实现 Sparrow

近日，在数据安全行业布局深久的 Google 率先发布了致力于保护嵌入式智能设备的操作系统 KataOS，这是对通用开源芯片上新的嵌入式安全操作系统的早期探索。KataOS 操作系统可能不适用于台式机或智能手机，但是对于智能家居等物联网设备具有良好的适配性。系统开发目标是为嵌入式硬件或边缘设备构建可验证的安全系统。KataOS 选择了 seL4 作为微内核，该内核主打数据安全保护，将安全性放在首位。

https://www.secrss.com/articles/48023

4、迈向量子安全时代，万事达卡推出抗量子非接触式支付卡

近日，金融服务巨头万事达卡（Mastercard）开发了一种新型非接触式卡，该卡结合了量子密码技术，旨在防止当前经典计算机和未来量子计算机的黑客攻击。万事达卡长期以来一直在探索量子计算的潜在影响，并于 2021 年 1 月推出了抗量子增强型非接触式规范。

此次发布的新卡旨在与所有现有终端配合使用，并带有量子加密算法来保护交易。它使用 EMVCo 最近披露的标准，即《EMV 非接触内核规范》：该规范可与所有现有的支付终端配合使用，同时还提供更高的安全级别。新规范的主要特点包括一个安全通道，用于保护隐私、防止窃听和保护敏感数据免受中间人和中继攻击。它还包括用于认证的椭圆曲线加密法，以及对生物识别和移动验证方法的支持。据支付商称，它将配备新一代算法和加密密钥，其设计速度很快，确保非接触式支付在半秒内完成，同时加强隐私保护，减少消费者设备和商家终端之间共享的账户信息。

当量子计算技术达到“量子优势”时，量子机器可以运行经典计算机不可能完成的近乎无误的计算，它也将使目前的密码学解决方案容易被破解，这意味着将需要特定的量子安全：专家预计这一点将在 2025-2027 年达到。**因此，预计到 2027 年，将有超过 125 亿台非接触式支付设备投入使用，**

使用这些设备进行的交易将在全球超过 10 万亿美元。

https://www.anquanke.com/post/id/281607

5、多因素身份验证（MFA）疲劳攻击呈上升趋势

长期以来，凭据泄露一直是网络入侵的主要原因之一，这也促使更多的组织采用多因素身份验证（MFA）作为防御手段。

过去，攻击者绕过多因素身份验证的主要方式是通过恶意软件或中间人网络钓鱼攻击框架（例如 evilginx2）窃取 cookie。然而，最近一种称为“MFA 疲劳攻击”的社会工程技术在黑客攻击中变得越来越流行。

MFA 疲劳攻击指的是攻击者运行一个脚本，自动反复使用被盗凭据登录，从而导致向帐户所有者的移动设备无休止地发送 MFA 授权通知。攻击者的目的是通过无休止的消息推送实施“疲劳轰炸”，击垮目标的安全意识，直至其出现失误。

在很多情况下，攻击者会反复推送 MFA 通知，然后通过电子邮件、消息平台或电话联系目标，甚至伪装成 IT 技术支持人员以说服用户确认 MFA 授权通知。最终，目标不胜其扰，忙中出错或者不小心误按“批准”按钮。

这是一种简单但有效的技术，目前已成功应用于针对

Microsoft、Cisco 和 Uber 的攻击案例中。

https://www.freebuf.com/news/346956.html

业界观点

1、冯登国院士：关键信息基础设施安全保护的三个视角

《关键信息基础设施安全保护条例》（以下简称《条例》）的意义和价值毋庸置疑，但是，《条例》要真正落地还任重而道远。同时，随着技术的发展、社会的进步，还要不断地研究完善《条例》，使它更加具有科学性和合理性。

当前，关键信息基础设施面临的安全问题主要表现在三个方面。

第一是产业链、供应链安全。从现在的形势来看，关键信息基础设施的产业链、供应链安全是当前最大的安全问题，也是当前产业界的痛点难点。有些关键信息产品或组件，一方面，面临着国外技术断供或垄断的风险；另一方面，这些产品或组件也存在被植入病毒、木马等恶意软件的风险。

第二是自身安全。关键信息基础设施自身的安全性非常重要，因为大部分关键信息基础设施要对外提供服务，如果自身难保，就不可能有效地提供服务，安全更无从谈起。

第三是应用安全。关键信息基础设施的一个重要作用是

给社会提供各式各样的应用服务，这就会产生应用安全问题。关键信息基础设施的应用安全是一个大概念，例如数据的安全问题、资源的安全问题、敏感信息的安全问题，还有国家和社会组织面临的安全威胁。

https://www.secrss.com/articles/48053

2、国家发改委张志华:“东数西算”工程初见成效

近日，国家发展改革委举行重大基础设施建设专题新闻发布会,介绍重大基础设施建设有关情况。国家发展改革委创新和高技术发展司副司长张志华介绍,今年 2 月,国家发展改革委会同中央网信办、工业和信息化部、国家能源局等部门,启动实施了“东数西算”工程,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,设立 10 个国家数据中心集群,正式拉开了构建全国一体化大数据中心体系的大幕。半年多来,“东数西算”工程初见成效。

张志华介绍到,一方面,重大工程加快建设。8 个国家算力枢纽所在地方政府高度重视,建立了工作协调推进机制,印发枢纽节点建设方案,细化工作目标、主要任务和时间节点,重点推进枢纽节点起步区建设。目前，8 个国家算力枢纽节点建设方案均进入深化实施阶段，起步区新开工数据中心项目

达到 60 余个，新建数据中心规模超过 110 万标准机架，项目总投资超过 4000 亿元,算力集聚效应初步显现。特别是，西部地区数据中心占比稳步提高，全国算力结构逐步优化。

张志华表示,下一步,国家发展改革委将会同有关部门,立体化推动“东数西算”工程,重点强化 4 个协同。

一是强化重大工程项目与配套政策的协同。进一步加强数据中心工程建设与用网、用地、用能、用水等配套政策同步落实,推动重大工程项目尽早建成应用。

二是强化多种政策工具间的协同。统筹用足用好中央预算内投资、各类金融工具、单列能耗等政策手段,支持国家算力枢纽和国家数据中心集群早日发挥作用。

三是强化国家算力枢纽与全国一体化算力网络体系的协同。在已布局国家算力枢纽基础上,统筹推进算力供给站、网络试验线、算力调度网、数据要素场、安全防护盾的一体化建设,构建覆盖全国、多层联动的算力网络体系。

四是强化数据中心建设与算力产业发展的协同。以国家算力枢纽和数据中心集群为引领,在规模化集聚算力和丰富场景应用的基础上,推动产业上下游协同发展,共同打造计算产业生态体系。

http://www.ciia.org.cn/news/19339.cshtml

3、王建冬：数据要素市场化配置水平仍待提升

数据要素市场建设过程中面临哪些问题和挑战？未来数据交易市场体系将呈现何种格局？构建全国统一的数据要素市场体系应如何发力？国家信息中心大数据发展部规划处处长、粤港澳大湾区大数据研究院院长王建冬表示，我国数据要素市场化配置水平总体还有待提升，主要体现在四个方面：

首先是顶层统筹力度有待加强。跨区域、跨部门、跨层级的协调机制和统一规范的数据流通规则尚未建立，“专网林立”“信息孤岛”“数据烟囱”等现象仍然存在。

其次在体制机制方面，数据产权不明、定价机制不清、流通机制不畅、公共数据开放应用水平较低等问题依旧突出，数据要素配置和收益分配机制有待完善。**再次，在数据要素市场生态体系方面，**数据交易场所的互联互通机制尚未形成，数据登记、合规公证、数据经纪、安全审计、资产评估、争议仲裁等面向数据要素市场需求的专业第三方服务生态体系有待建立。此外，**国际数字环境日趋复杂，**国际上数据保护主义、数据霸权主义抬头，我国面临全球数据要素治理的重要课题。

王建冬称，可从多方面发力构建全国统一的数据要素市场体系，主要包括加强数据要素基础设施和标准规范建设、

强化公共数据共享开放和新技术应用、发挥政府引导作用促成产业集聚优势、创新完善监管体制机制和信用体系建设以及积极开展数据跨境流通试点示范工程。

https://mp.weixin.qq.com/s/SezmhRKJJubUa36cDezSCg

4、CISA 专家：让多因素成为默认选项，而不是消费者的选择

安全从业人员长期以来一直在吹捧多因素身份验证，其中任何登录系统的人都必须提供除密码之外的其他合法性证据，例如一次性密码。尤其是当绑定到硬件 fob 时，多因素使黑客更难渗透系统。但是多年来 MFA 并没有转化为广泛采用。

美国网络安全和基础设施安全局局长 Jen Easterly 提出一个解决方案：让多因素成为默认选项，而不是消费者的选择。供应商应该“强力推动”用户使用 MFA，并为需要它的用户提供更完整的功能集。她还呼吁“彻底透明”，称供应商应公布 MFA 采用率，特别是对于系统管理员等特权用户。

网络安全和基础设施安全局高级技术顾问 Bob Lord 表示，微软是仅有的几家发布了有关 MFA 使用信息的公司之一。这家西雅图地区的软件巨头发现，只有五分之一的用户采用了 MFA。Lord 将这种情况比作 1970 年代的安全带，

当时大多数车辆都有安全带，但只有少数司机和乘客佩戴。“可用性是不够的，”Lord 说。“我们看到太多组织失败的部分原因是他们不知道他们需要做 MFA。那是因为他们没有东西可以推动他们朝着正确的方向前进。”

https://www.govinfosecurity.com/us-cisa-official-forcefully-nudge-users-to-adopt-mfa-a-20286

5、隐私观点：消费者表示信任取决于透明度

近日的“思科 2022 年消费者隐私调查”收到了来自 12 个国家/地区的 2,600 份匿名回复，获得了以下发现:

1）信任取决于透明度。调查发现，39% 的受访者选择“数据透明度”作为组织在如何使用和保护个人数据方面建立信任的首要任务。

2）消费者采取行动保护数据。37%的受访者已经采取了更困难的步骤来结束与公司或提供商的关系。

3）对 AI 应用程序的混合支持和关注。43% 的受访者表示人工智能有助于改善他们的生活，54% 的受访者甚至愿意分享他们的匿名个人数据以改进人工智能产品。然而，60% 的人担心企业今天如何使用人工智能，65% 的人表示，由于他们的人工智能实践，他们已经失去了对组织的信任。

对此，调查者对相关组织提出以下建议:

1）投资于透明度。向您的客户展示他们可以在哪里找到您公司的隐私政策，并以易于理解的方式告诉他们您如何使用他们的数据，因为这对于赢得和建立他们的信任至关重要。

2）帮助确保您的客户了解相关的隐私法及其权利。了解这些保护措施的个人更有可能信任组织的个人数据，并相信他们的数据受到保护。

3）采取措施确保负责任地应用和使用人工智能。根据这项研究，负责任地应用和使用人工智能的积极步骤包括实施人工智能治理框架，提供关于人工智能如何在产品和服务中应用和使用的透明度，以及使客户能够选择退出特定应用程序。

4）评估数据本地化要求的成本和法律替代方案（如果有）。对于许多消费者来说，这些要求可能不值得他们付出代价，而且尚不清楚它们是否有助于提高安全性和隐私性。

https://iapp.org/news/a/consumers-say-trust-depends-on-transparency/

数据安全事件

1、微软数据泄露暴露全球 111 个国家超 6.5 万实体的客户个人信息

10 月 19 日报道，微软表示，由于一台服务器配置不当，导致某些客户的敏感信息遭暴露。

微软在 2022 年 9 月 24 日获悉该泄露事件后加固了服务器安全，“配置不当可导致对微软与客户之间的某些企业交易数据的未认证访问权限。经过调查未发现客户账号或系统受陷。我们已直接告知受影响客户。”

威胁情报公司 SOCRadar 声称发现微软的服务器泄露了 2.4TB 的数据，包括超过 335000 封电子邮件、133000 个项目和 548000 个暴露的用户，还有 SOW 文档、产品报价、POC 和 POE 文件等。泄露数据与 111 个国家的 65000 多个组织有关，存储了 2017 年至 2022 年 8 月的信息。

https://www.bleepingcomputer.com/news/security/microsoft-data-breach-exposes-customers-contact-info-emails/

2、黑客称他们从英国一保险公司窃取了 1.4TB 数据

10 月 18 日，据外媒报道，勒索软件组织 LockBit 声称他们破坏了英国保险公司 Kingfisher Insurance 以及该公司

的汽车保险品牌 First Insurance 的服务器，窃取了包括员工和客户的个人详细信息。

根据 LockBit 泄密网站上的帖子，该数据集包括员工和客户的个人数据以及联系人和公司邮件档案。黑客声称他们已经从保险公司收集了 1.4 TB 的数据。

https://cybernews.com/news/hackers-stole-data-from-kingfisher-insurance/

3、澳大利亚零售巨头泄露 220 万用户数据，并被黑客在线出售

10 月 17 日，据 Security affairs 等网站消息，澳大利亚零售巨头 Woolworths 批露了近期旗下子公司 MyDeal 一起影响 220 万用户的数据泄露事件，攻击者已在黑客论坛上发帖出售被盗数据。

据称，攻击者通过利用用户泄露的凭据获得了对 MyDeal 客户关系管理 (CRM) 系统的访问权限。泄露的客户数据包括姓名、电子邮件地址、电话号码、送货地址，对于某些个人，还包括出生日期。付款、驾驶执照或护照详细信息被访问。该公司已经联系了所有受影响的客户。

https://securityaffairs.co/wordpress/137262/data-breach/woolworths-data-breach.html

4、Meta Pixel 导致的卫生系统数据泄露影响 300 万患者

10 月 20 日，据外媒报道，威斯康星州和伊利诺伊州拥有 26 家医院的医疗保健系统 Advocate Aurora Health (AAH) 正在通知其患者一起数据泄露事件，该事件暴露了 3,000,000 名患者的个人数据。

该事件是由于在 AAH 网站上对 Meta Pixel 的不当使用造成的，患者在该网站上登录并输入敏感的个人和医疗信息。

Meta Pixel 是一种 JavaScript 跟踪器，可帮助网站运营商了解访问者如何与网站互动，从而帮助他们进行有针对性的改进。然而，跟踪器也会将敏感数据发送到 Meta (Facebook)，然后与庞大的营销网络共享，这些营销网络针对患者投放与其病情相匹配的广告。

这一隐私泄露事件已席卷美国，因为该国许多医院都在使用 Meta Pixel，将数百万人暴露给第三方，并引发针对相关组织的集体诉讼 。

https://www.bleepingcomputer.com/news/security/health-system-data-breach-due-to-meta-pixel-hits-3-million-patients/?&web_view=true

5、葡萄酒在线零售商 iDealwine 遭遇数据泄露

10 月 19 日，据外媒报道，受欢迎的国际精品葡萄酒在线零售商 iDealwine 在上周末遭遇数据泄露，尚未透露受影响的客户数量。

它的电子商店仍处于离线状态，只显示一条简短的解释性消息，目前该公司已通过电子邮件及博客通知所有可能受影响的客户有关网络攻击的信息。根据通知，客户的姓名、地址、电话号码和电子邮件地址可能已被泄露，客户的信用卡/银行信息没有被泄露，因为它没有存储在公司服务器上。

https://www.helpnetsecurity.com/2022/10/19/idealwine-data-breach/?web_view=true

6、Cybernews 研究团队发现数百万个公开的 .git 文件夹

10 月 20 日报道，Cybernews 最近的另一项研究发现，总部位于美国的流媒体服务 CarbonTV 将服务器的源代码开放，从而危及用户安全和公司声誉。由于对 .git 文件夹的访问控制不佳，而导致源代码泄漏。

Cybernews 的研究人员在最常见的 Web 服务端口 80 和 443 上发现了 1,931,148 个 IP 地址，这些 IP 地址具有可供公众访问的 .git 文件夹结构的实时服务器。超过 31% 的公开 .git 文件夹位于美国，其次是中国 (8%) 和德国

(6.5%)，大约 6.3% 的公开 .git 配置文件在配置文件本身中有部署凭据。

https://securityaffairs.co/wordpress/137371/security/millions-git-folders-exposed-public.html?web_view=true

7、零售巨头 Woolworths 披露 MyDeal 在线市场的数据泄露

10 月 17 日，据外媒报道，澳大利亚零售巨头 Woolworths 披露了一起影响大约 220 万 MyDeal 客户的数据泄露事件。

攻击者通过利用用户泄露的凭据获得了对 MyDeal 客户关系管理 (CRM) 系统的访问权限。泄露的客户数据包括姓名、电子邮件地址、电话号码、送货地址，对于某些个人，还包括出生日期。

https://securityaffairs.co/wordpress/137262/data-breach/woolworths-data-breach.html

8、谷歌在未经同意的情况下收集生物特征数据

10 月 20 日，得州检察长起诉 Google，指称这家搜索巨头在未征得用户完全同意的情况下收集脸部和语音特征等生物识别数据，违反了该州的生物识别隐私法（又名生物识别标识符的捕获或使用法）。根据在得州米德兰县州立地区

法院提交的诉状，得州称 Google 的数据收集行为可追溯至 2015 年，影响了该州数百万居民。

https://www.bleepingcomputer.com/news/security/google-sued-over-biometric-data-collection-without-consent/

9、澳大利亚健康保险公司遭勒索攻击，200GB 客户数据被盗

澳大利亚健康保险公司 Medibank 开始通知客户称，他们的个人数据可能在最近发生的一次网络攻击中被盗。

当地时间 10 月 12 日，该公司披露称遭勒索攻击就某些系统因此下线。被盗的个人信息包括全名、地址、出生日期、电话号码、医疗号码和保单号码以及索赔数据（如客户接受医疗服务的地址）。

https://www.secrss.com/articles/48178

10、黑客窃取了伊朗原子能机构的敏感数据

10 月 23 日，伊朗原子能机构声称，由国家资助的黑客入侵了其电子邮件系统。自称为 Black Reward 的黑客组织在 Telegram 上宣布了对原子能组织的黑客攻击，并分享了有关布什尔工厂的合同、建设计划和设备细节的文件，作为入侵的证据。该组织宣布泄露了 50 GB 的敏感文件，目前尚不清

楚海量数据是否还包含机密信息。
https://securityaffairs.co/wordpress/137513/hacking/hackers-stole-sensitive-data-from-irans-atomic-energy-agency.html

11、Vice Society 声称已窃取法国某医院的 150 GB 文件

据 10 月 19 日报道，法国一家私立妇产医院 Hôpital Pierre Rouquès-Les Bluets 遭到攻击。攻击发生于 10 月 9 日，该医院在其网站主页上披露了此次攻击，并表示邮件系统无法正常工作。Vice Society 黑客组织声称他们已攻击该医院，并加密了医院的所有文件和备份，尽管医院表示大多数医疗记录仍然可以访问。此外，他们还从医院的系统中下载了超过 150 GB 的文件。
https://www.databreaches.net/french-maternity-hospital-hit-by-ransomware-attack-by-vice-society-attackers-claim-to-have-150-gb-of-files/

《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/