全球数据安全观察

总第 112 期 2022 年第 40 期

(2022.10.31-2022.11.06)

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、国务院：全面加强网络安全和数据安全保护

10 月 28 日，国务院关于数字经济发展情况的报告提请十三届全国人大常委会第三十七次会议审议。

报告提出，**以数据为关键要素**，以推动数字技术与实体经济深度融合为主线，以协同推进数字产业化和产业数字化、赋能传统产业转型升级为重点，以加强数字基础设施建设为基础，以完善数字经济治理体系为保障，不断做强做优做大我国数字经济。并在下一步工作安排中明确指出要“**全面加强网络安全和数据安全保护，筑牢数字安全屏障**”。

http://www.news.cn/fortune/2022-10/28/c_1129086321.htm

2、工信部发布《道路机动车辆生产准入许可管理条例（征求意见稿）》

10 月 28 日，工业和信息化部会同有关部门发布《道路机动车辆生产准入许可管理条例（征求意见稿）》。条例将“生产智能网联汽车企业同时应当具备车辆产品网络安全、数据安全保障能力”列为申请道路机动车辆生产企业准入许可条件之一；将“智能网联汽车产品同时应当符合预期功能安全、功能安全、网络安全和数据安全相关标准、技术规范要求”列

为申请道路机动车辆产品准入许可条件之一。

https://www.miit.gov.cn/jgsj/zbys/qcgy/art/2022/art_35882ca7a3c044e587037f2c34c524f9.html

3、国家网信办依法集中查处一批侵犯个人信息合法权益的违法违规 App

近期，针对人民群众反映强烈的 App 以强制、诱导、欺诈等恶意方式违法违规处理个人信息行为，国家网信办依据《个人信息保护法》《App 违法违规收集使用个人信息行为认定方法》等法律法规规定，依法查处“超凡清理管家”等 135 款违法违规 App。

https://mp.weixin.qq.com/s/jJgQfK2VyAXkl-F4vtUaeQ

4、西安市印发《西安市“十四五”数字经济发展规划》

10 月 28 日，《西安市“十四五”数字经济发展规划》经市政府同意印发。

规划提出“在确保数据安全、保障用户隐私的前提下，调动行业协会、科研院所、企业等多方参与数据价值开发”，并“在保护个人隐私和确保数据安全的前提下，探索将个人数据服务纳入数据要素市场体系，推动有序流通应用”。同时明确“完善数据安全治理体系，建立数据分类分级保护制度，推动

数据全链条相关责任主体落实数据安全保护责任”的强化安全保障要求。

http://www.xa.gov.cn/gk/zcfg/szbf/6360eba3f8fd1c4c2124f1e1.html

5、《信息技术 大数据 政务数据开放共享 第 4 部分：共享评价》发布

近日，《信息技术 大数据 政务数据开放共享 第 4 部分：共享评价》（GB/T 38664.4-2022）获批发布，将于 2023 年 5 月 1 日正式实施。

该标准主要包括范围、规范性用文件、术语和定义、评价内容和要求、评价方法等内容，旨在推进政务数据高效有序共享，深化政务数据开发利用，提升政务数据共享的规范性、实效性和创新性，评价指标体系主要包括 5 项一级指标、22 项二级指标和多项三级指标，各级指标权重可根据各地、各部门实际情况进行动态调整。

https://mp.weixin.qq.com/s/AEqOhPI2vz8r5K-ZwiaD2g

6、中国信通院牵头的联邦学习评估方法国际标准在 ITU 立项成功

2022 年 10 月 17 日至 2022 年 10 月 28 日，国际电信联

盟第十六研究组（简称 ITU-T SG16）召开全体会议，由中国信通院云计算与大数据研究所牵头的联邦学习国际标准《Assessment criteria of federated learning platforms》立项成功，该标准可以指导联邦学习相关的实践方怎样以合理地方式评估联邦学习平台及主要的联邦学习算法。

https://mp.weixin.qq.com/s/AsXg4jZ7kpXpCX2n1O2WWg

技术、产品与市场

1、欧盟委员会推出首个欧盟 GDPR 认证机制

近期，欧盟委员会推出了首个获批的欧盟通用数据保护条例（GDPR）认证体系——Europrivacy（欧洲隐私）。这一数据保护标记最近还获得了欧洲数据保护委员会的批准，象征着欧盟在推动隐私保护规则上又向前迈进了一大步。

Europrivacy 作为第一个符合 GDPR 规定的官方认证机制，是一项由欧洲研究项目(ERP)，根据 ISO/IEC 17065 和 GDPR 第 42 条的基础而研究开发的认证计划，用于评估、记录、认证和评价企业对GDPR等数据保护法规的合规情况。经评估后符合这一标准的认证对象，证书中可以获得欧洲数据保护印章。

该认证体系本身为混合模式，配备了许多领域的数据处理功能，几乎适用于所有数据处理活动，包括了人工智能，区块链，电子健康和物联网等创新技术。除了证明 GDPR 的合规性外，Europrivacy 还可用于评估跨境数据传输的充分性或帮助选择数据处理器。

https://www.secrss.com/articles/48524

2、美国财政部：2021 年金融机构因勒索攻击损失超 12 亿美元

安全内参 11 月 2 日消息，美国金融监管机构发布报告称，**2021 年勒索软件攻击与赎金支付数量再创历史新高**，多数勒索软件变种的幕后操纵者据信与俄罗斯有关。

总体来看，**2021 年金融机构根据美国《银行保密法》要求上报的勒索攻击总损失，已经由前一年的 4.16 亿美元骤升至 12 亿美元**，翻了近 2 倍。

2021 年内上报事件总计 1489 起，远高于 2020 年的 487 起。研究人员报告称，“勒索软件持续对美国各关键基础设施部门、企业及公众构成重大威胁。”

https://www.secrss.com/articles/48587

3、聚焦 XR 技术：隐私未来论坛发布“数据流动和隐私风险”信息图

全球非营利组织隐私未来论坛（Future of Privacy Forum，简称“FPF”）发布了其关于 XR 技术的数据流动和隐私风险信息图，通过探索 XR 技术可能支持的用例，将 XR 数据流动的工作方式、利用的传感器种类、数据类型、数据处理和传输流程可视化。

随着企业越来越多地开发和采用虚拟(VR)、混合(MR)和

增强(AR)现实等拓展现实（XR）技术，潜在的隐私和数据风险与日俱增。立法者、监管机构和其他专家对 XR 技术的工作原理、数据保护风险以及可采保护措施来越来越感兴趣。

XR 技术由多个传感器、大量数据以及各种算法和自动化系统（例如机器学习）的相互作用提供支持。然而，**这些用例通常依赖于可能属于敏感个人数据的信息，而这些数据的收集、处理和传输可能会给用户和旁观者带来隐私和数据保护风险。**

https://www.secrss.com/articles/48527

4、研究：制造和生产行业勒索软件受害者支付的赎金最高

根据网络安全公司 Sophos 的研究调查，制造和生产行业中勒索软件攻击的受害者支付的赎金数额最大，支付的平均赎金要求超过 200 万美元。

在支付赎金的人中，37%的受访者最终支付了超过 100,000 美元，而 8% 的人支付了超过 100 万美元的解密密钥。但是，虽然受害者可能认为支付赎金要求是恢复数据的最快方式，但根据对制造和生产部门事件的分析，在支付赎金后平均只有 59% 的数据被恢复。

制造业对于勒索软件团伙来说是一个诱人的目标，因为它在供应链中扮演着重要角色——制造工厂长时间处于离

线状态将导致非常昂贵的代价，并对其他行业、企业和消费者产生连锁反应。

https://mp.weixin.qq.com/s/6rDn1ZVfXpxm3aJOJwOXcA

5、IDC：上半年数据复制与保护市场规模达 2.7 亿美元 同比增长 9.8%

据 IDC 发布《中国数据复制与保护系统市场季度跟踪报告，2022 上半年》显示，2022 上半年，数据复制与保护市场较去年同期实现了 9.8%的增长，市场规模达到 2.7 亿美元。

IDC 预测，未来五年，中国数据复制与保护市场将以 13.7%的年复合增长率(CAGR)增长，在 2026 年达到 12.6 亿美元。其中备份一体机将在 2022 年保持健康增长，未来五年将保持 12.7%的年复合增长率。数据复制与保护软件市场凭借在数据治理和全生命周期管理方面价值，将继续保持高速增长，在未来五年的复合增长率将高于备份一体机市场达到 15.2%，市场规模也将在 2026 年达到 5.4 亿美元。

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

业界观点

1、肖远企：强化金融科技监管建设 加强金融消费者权益和数据安全保护

10 月 31 日，中国银保监会副主席肖远企出席“香港金融科技周 2022”发表演讲。他强调，在金融科技发展同时，要不断强化金融科技监管建设，完善监管规则和机制，丰富监管方式和手段，确保金融科技安全稳健发展。

一是**完善基于规则的监管**。坚持金融业务必须持牌经营的原则，将所有金融活动纳入金融监管，持续完善修订现行金融监管规定，针对新兴的金融科技活动及时制定出台专门审慎监管规则。

二是**丰富金融科技监管工具**。在监管科技方面，持续推进现场检查和非现场监测的数字化体系建设。在合规科技方面，鼓励金融机构积极探索建设数字化平台，强化对合规风险的有效管控。

三是**加强消费者保护**。要非常关注金融科技及其创新对公众利益的影响。在金融科技发展的进程中，加强金融消费者权益和数据安全保护、强化信息披露同样至关重要。

http://insurance.hexun.com/2022-11-03/207037371.html

2、蒋宁：聚焦开放金融生态下的数据价值释放

目前隐私计算虽已成功解决一些金融场景下的数据合规问题，但其在安全、性能、互联互通等方面仍存在巨大挑战，可能限制进一步的推广和应用。对此，蒋宁认为可以在以下方面做进一步提升。

通过软硬件优化加速提升隐私计算可用性。隐私计算底层的密码学技术虽带来了安全性，但计算效率被大大降低。因此，为满足未来的规模化落地，隐私计算平台需进行大量优化，针对数据处理各个环节，将性能提升到最优，并研究高性能硬件，以满足隐私计算的实时性要求。

隐私计算与多种技术互相融合。隐私计算与区块链、同态加密、差分隐私等技术将逐步融合，发挥技术的最大价值，并拓展应用场景边界。例如，区块链与隐私计算的结合，可实现全闭环的安全和隐私服务。

隐私计算行业生态的融合发展。当前虽已有成功的隐私计算案例，但多数仍处于摸索实验阶段，还未形成规模化效应。产学研用各界需加强隐私计算相关研究、开发、应用的布局。越来越多的开源项目也将加速隐私计算技术迭代，降低开发门槛和成本。隐私计算未来将形成多元、开放的产业生态。

http://finance.ce.cn/home/jrzq/dc/202211/04/t20221104_382113

85.shtml

3、如何在 60 分钟内快速应对数据泄露

有数据显示，企业平均需要 287 天才能发现数据泄露。发现泄露所花的时间越长，对公司造成的损害就越大。因此，尽快发现泄露至关重要。

企业常见的数据泄露类型，主要包括：未经授权的非法访问、被越权查看的机密数据、将敏感数据错误发送给收件人、重要数据存储设备被盗、重要数据被篡改、数据信息丧失可用性（比如勒索软件攻击）。

常见的数据泄露特征包括：发现企业的机密信息在网上泄露、发现有未经授权的企业网络下载记录、发现有人打开了来源不明的邮件附件、发现有异常的远程位置登录企业网络、异常的时间段出现了来自标准账户和特权账户的活动、发现企业的系统日志被篡改、多起 DDoS 攻击让安全团队无暇顾及实际攻击。

一旦发现遇到数据泄露，可以采用以下列方式在 60 分钟内快速处理与响应：

提醒员工。如果发现数据泄露切莫恐慌，尽快通知员工并向他们说明情况，指示他们在数据泄露后应如何应对，例如讲明如何与客户沟通、如何回应其他员工等。

评估风险和优先级。确定数据泄露的根源，找出哪些数据受到了影响。首先，准确评估泄露的数据，切忌空泛，比如“我们所有的客户数据都面临风险”。其次，确定数据泄露给企业和客户带来的风险。如果风险过高，就需要停止业务运营，直到消除风险。

遏制泄露。具体情况评估完成后，需要从系统中移除所有受影响的部件，包括受攻击影响的计算机、笔记本电脑、服务器或其他任何设备。从泄露的数据中寻找共同点。这可能表明数据泄露的单一来源，也可能表明泄露的单一方法。

保护与泄露相关的物理区域。下一步是保护与泄露相关的物理区域，把它们封锁起来。在问题解决之前除了应急团队外，其他人员一概不得访问。此外，还可以询问取证分析专家和执法人员何时恢复正常操作。

详细记录。务必要把与与数据泄露相关的一切记录下来:从最初发现泄露，到为处理泄露所采取的每一步。还应该保存与员工、客户或执法机构之间的通信记录。除了提供准确信息外，详细记录对于企业在提交报告时也大有帮助。

防范进一步的数据泄露。最后，采取必要的措施以预防进一步的数据泄露。这包括移除含有安全漏洞的第三方软件。此外，彻查数据安全系统，找出任何潜在的安全漏洞，一旦发现立即处置。还应该查找任何已经泄露的数据，比如客户

信息、财务记录或公司数据。采取必要措施将这些数据从网上删除。此外，即使在遏制数据泄露之后，也必须保持警惕。因为永远无法确定这是孤立的事件，还是一起针对企业的更广泛的恶意活动的一部分。

https://www.aqniu.com/homenews/90611.html

4、数据合规与企业发展如何平衡？

如果说，互联网三十年，前半程是狂奔，后半程则是合规。对于企业未来的数据合规路径，专家与企业从不同角度，表达了不同的思路。

郭金龙认为，作为互联网创业者，应加强合规审查，避免因商业模式创新而带来的潜在法律风险，降低因不合规而造成创业项目失败的风险。企业在经营活动中，应当认真进行合规论证，避免落入恶意竞争的规制范围。

王伟表示，企业应当根据《民法典》、《个人信息保护法》、《数据安全法》等相关法律，构建完善的个人信息保护合规管理机制，在展业、销售、财务、物流、客服等各个环节保护好个人信息。通过建立严格的合规准则和标准、合规审查、合规风险预警、投诉处理、反欺诈反舞弊、合规问责等机制，并将其嵌入各个业务环节、重要业务系统，是防范违规风险的重要路径。

李兰兰建议，在兼顾合规成本与法律风险防范的前提下，企业可以根据自身的实际情况分版块、分步骤、分阶段开展合规建设，从核心业务如 APP 合规、数据交易合规、产品开发合规、平台建设合规、数据出境合规等“专项合规”开始做起，然后再慢慢扩大至其他业务线和整体合规体系建设。

http://www.21jingji.com/article/20221105/herald/4c847b2911cef912ea1d788003b289c3.html

5、敏感个人信息提示不充分，外部监督机制待完善

2021 年 11 月 1 日，《个人信息保护法》正式施行，转眼间即将实施一周年。中国社会科学院法学研究所与南方财经全媒体集团共同组成课题组研发“守门人”社会责任指标体系，从制度体系建设、组织架构、合规实践、平台治理与社会责任报告五个维度对 18 家大型平台企业的代表性 APP 做出测评，根据公开的可查询渠道，严格依据指标，对这些“守门人”平台的社会责任履行情况做出判断。

测评结果显示，所有 APP 均在隐私政策中按照提供服务类型的不同对采集的个人信息种类进行了分类，较为清晰地列举了用户使用何种功能所需的个人信息类型；大部分平台都提供了隐私政策概要或个人信息采集清单等易于理解的形式，简单、直观地体现收集和使用个人信息的类型和场景。

但普遍来看，相关工作仍有较大的提升空间。部分 APP 隐私政策中并未明确区分或说明采集敏感个人信息；在获取用户身份信息、人脸信息等相关敏感信息时单独同意的提醒方式不够显著，或存在未进行提示的情况；对用户的敏感个人信息有单独同意的程序设置，但是对于平台内经营者的个人敏感信息采集存在不够规范提示的情况。

从目前测评结果来看，平台绝大部分已在内部建立专门的个人信息管理部门，统筹相关合规事宜，且在隐私政策或官网等渠道给出相关部门的联系方式，用户可通过联系主管部门或客服渠道实现对个人信息权利的行使。

但从测评结果也指出，目前大部分 APP 隐私政策所公示出的个人信息保护负责人大部分均未明确其身份或职务，联系方式大部分为部门电话或邮箱，用户无法获知负责人的具体信息和其对自己个人信息承担的责任，相关公示内容有待进一步完善补充。

在独立监督架构方面，同样存在不少问题。仅有个别平台企业对外表明，已开展外部独立监督机构建设，且就测评团队与企业、研究机构等相关单位交流结果看，目前关于外部独立监督机构在人员选择、组织架构等方面仍未有细则标准。

在已经公开表示将会设立外部监督机构的企业（微信、

携程），目前也尚未有进一步动态，关于监督机构成员的选聘过程、人员构成比例、具体工作内容，或许需要更为明确的监管规则或业界实践加以指引。

http://www.21jingji.com/article/20221101/herald/6be1656c89b1ad830ab0073ff1fd9000.html

数据安全事件

1、OPERA1ER 团伙已从银行和电信公司窃取超过 1100 万美元

据 Group-IB 11 月 3 日称，黑客团伙 OPERA1ER 利用现成的黑客工具，已从银行和电信服务提供商窃取了至少 1100 万美元。除了主要针对非洲的公司外，该团伙还攻击了阿根廷、巴拉圭和孟加拉国的组织。从 2018 年到 2022 年，黑客总共发起了超过35次成功的攻击,其中约三分之一是在2020年进行的。OPERA1ER 利用鱼叉式钓鱼攻击获得初始访问权限，主要依靠开源工具、商品恶意软件以及 Metasploit 和 Cobalt Strike 等框架来入侵公司的服务器。
https://blog.group-ib.com/opera1er-apt

2、Dropbox 遭到钓鱼攻击导致 130 个 GitHub 存储库泄露

Dropbox 在 11 月 1 日透露，黑客使用钓鱼攻击中获得的员工凭证访问其一个 GitHub 帐户后窃取了 130 个代码存储库。该公司于 10 月 14 日发现攻击者入侵了该帐户，此次攻击针对多名 Dropbox 员工，通过冒充 CircleCI 的邮件将他们重定向到钓鱼页面，并要求他们输入 GitHub 凭据。该公司称，受影响存储库包括其为 Dropbox 使用而稍作修改的第三方库副本、内部原型以及安全团队使用的一些工具和配置文

件，并不包含核心应用程序或基础设施的代码。

https://www.bleepingcomputer.com/news/security/dropbox-discloses-breach-after-hacker-stole-130-github-repositories/

3、沃达丰意大利公司披露其经销商被黑导致的数据泄露事件

据 11 月 2 日报道，沃达丰意大利公司（Vodafone Italia）通知其客户关于经销商 FourB SpA 被黑导致的数据泄露事件。攻击发生在 9 月的第一周，泄露了用户的详细信息，如订阅信息、身份证件和联系方式等。目前，FourB 已经关闭了对被入侵服务器的访问，并实施了更高级别的安全策略。2022 年 9 月 3 日，自称 KelvinSecurity 团伙曾声称攻击了 Vodafone Italia 并窃取了 295000 个文件，总计 310 GB 的数据。当时，沃达丰回应称其公司内部 IT 系统并未遭到未经授权的访问，但将继续调查。尚不清楚该事件是否与此次披露的泄露事件有关。

https://www.bleepingcomputer.com/news/security/vodafone-italy-discloses-data-breach-after-reseller-hacked/

4、黑客成功入侵乌军战场指挥系统，战场数据泄露

11 月 2 日报道，1 日晚间，黑客组织“Joker DPR”（顿

涅兹克小丑)在电报群宣称已成功入侵乌克兰武装部队(AFU)使用的所有军事指挥和控制程序，包括可接入北约 ISR 系统的美国 Delta 数字地图战场指挥系统，该系统目前是乌克兰部队主要使用的战场指挥系统。

此前，乌克兰媒体曾披露美国军方提供给乌克兰的先进军事技术和软件，其中就包括 Delta 战场指挥系统。**Joker DPR 在电报频道中宣称已经用病毒感染了所有接入 Delta 系统的计算机，并且篡改了其中的数据。**

https://southfront.org/us-delta-program-used-by-ukrainian-military-command-hacked-by-joker-dpr-hacker-team/

5、网站扫描引擎 Urlscan.io 的 API 无意中泄露了敏感的 URL 和数据

11 月 2 日，据外媒报道，由于第三方服务配置错误，公开列表使 urlscan.io 上的敏感数据可搜索。

Urlscan.io 是一个网站扫描和分析引擎。该系统接受 URL 提交并生成大量数据，包括域、IP、DOM 信息和 cookie，以及屏幕截图。Urlscan.io 支持许多企业客户和开源项目，并提供 API 将这些检查集成到第三方产品中。

据调查，本次事件与 urlscan.io 集成的安全编排、自动化和响应 (SOAR) 剧本配置错误有关。安全研究员检查了

urlscan.io 的历史信息，并发现了配置错误的客户端，这些客户端可能会通过从系统中抓取电子邮件地址并向其发送唯一链接以查看它们是否会出现在 urlscan 上而被滥用。

https://portswigger.net/daily-swig/urlscan-io-api-unwittingly-leaks-sensitive-urls-data?&web_view=true

6、泄露的 Amazon Prime 视频服务器暴露了用户的观看习惯

11 月 1 日，据外媒报道，安全研究员 Anurag Sen 透露亚马逊未能保护其内部服务器，这使得任何第三方都可以访问 Elasticsearch 数据库。

据称，该数据库存储在亚马逊内部服务器上，并包含 Prime Video 观看习惯。由于缺乏密码保护，该服务器可以在 Internet 上访问。因此，访问网络浏览器的人只需输入其 IP 地址即可访问可用数据。

暴露的数据库包含 2.15 亿条匿名观看数据记录，包括正在流式传输的电影或节目的名称、用于流式传输内容的设备以及类似的内部数据，例如订阅信息和网络质量。

https://www.hackread.com/amazon-prime-video-viewing-habits/?web_view=true

7、LockBit 勒索软件声称攻击汽车巨头 Continental

11 月 3 日，LockBit 勒索软件团伙声称对针对德国跨国汽车集团 Continental 的网络攻击负责。

据称，LockBit 还从 Continental 的系统中窃取了一些数据，如果该公司在接下来的 22 小时内不满足他们的要求，他们威胁要在他们的数据泄露网站上发布这些数据。

https://new.qq.com/rain/a/20221030A05GCR00

8、澳大利亚国防军通信服务平台遭到勒索软件攻击

11 月 1 日，外媒报道称澳大利亚军事人员和国防雇员使用的通信平台 ForceNet 疑似成为勒索软件的最新受害者。此次攻击始于 2022 年 10 月，但攻击并未破坏其防御 ICT 系统，数据也并未遭到泄露。据国防部部长助理称尽管此次攻击并未导致数据泄露，但会认真对待此次事件，并会将此次事件通知给所有人员。

https://www.secrss.com/articles/48251

9、台湾 2300 万人民信息泄露，黑客开价 5000 美元

11 月 1 日报道，近期，联合新闻网披露，有黑客在国外论坛 “BreachForums” 上出售 20 万条中国台湾省民众的个人资料，并声称拥有台湾省 2300 万民众的详细信息。

台湾省某部门接到举报后立刻展开调查，初步调查结果显示，在售的 20 万条信息所有者主要集中在宜兰地区，且信息全部吻合，县长林志妙、民进党立委陈欧珀的个人信息也在其中。该名黑客以 5000 美元（约 3.6 万人民币），将 2300 多万条数据 "打包 "出售，并强调可以用比特币支付。https://www.freebuf.com/news/348462.html

10、湖南一公务员非法获取公民个人信息 4 亿余条：非法获利 170 余万

日前，湖南省岳阳市中级人民法院对一起侵犯公民个人信息案中刑事附带民事公益诉讼部分作出驳回上诉，维持原判的终审裁定。该案中，钟某某利用自己所学专长，非法获取大量公民个人信息贩卖给诈骗集团牟利，不到一年的时间，非法获取公民个人信息 4 亿多条，通过虚拟货币交易获取非法收入 175 万余元。

汨罗市人民法院审理后作出一审判决，以侵犯公民个人信息罪判处钟某某有期徒刑三年六个月，并处罚金人民币 1759657 元。

案发前，钟某某是一名负责基层环境保护的公务员。2020 年 8 月，为批量获取公民个人信息出售获利，钟某某利用自己所学自制小程序，并购买源代码批量查询获取他人手

机号码对应的微信号、微信昵称、性别、实名认证信息、IP地址、微信群群名、群内成员微信号、入群方式、入群时间、退群时间等内容的公民个人信息。

https://www.secrss.com/articles/48689

11、查个表公民个人信息就被卖了！网警披露最新案例，水电公司有内鬼

今年的11月1日是《个人信息保护法》实施一周年，公安机关网安部门始终努力为个人信息安全保驾护航。近日，浙江宁波慈溪网警大队就侦破了一起侵犯公民个人信息的案件，作案主要方式竟然是查水表查电表。

网警调查发现，慈溪市某威不动产经纪有限公司可能存在非法获取公民个人信息的犯罪行为。业务员们为了获得精准客源，拓展业务，打听到某一套房的房东有出售意图，便去查询用户水电等装表信息，最终达到自己的营销目的。

经查证，犯罪嫌疑人杜某利用在供电所工作的便利，窃取并出售电力用户信息，私下帮助中介公司和个人查询“电表用户”信息，犯罪所得达三十余万元。目前，某威不动产经纪公司涉案人员，以及李某、杜某等10余人，均已被慈溪市公安局依法采取刑事强制措施。

https://mp.weixin.qq.com/s/GtVEmTlGXk5voP6-arPDAw

《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/