[公开]360NELab-DST-0-015-20201026

大数据协同安全技术
国家工程实验室
National Engineering Laboratory for Big Data Collaborative Security Technology

全球数据安全观察

总第 15 期 2020 年第 15 期

（2020.10.19-2020.10.25）

大数据协同安全技术国家工程实验室

摘要

本期全球数据安全观察搜集到的重要事件的主要类型可分为数据泄露、数据基础设施和个人隐私保护的发展以及因数据不合规的调查和罚款等。

在线游戏因严重漏洞造成 190 万用户信息泄露

五万多台家用摄像设备被黑客攻击，导致录像被公开

俄罗斯 APT 团体入侵了美国政府网络窃取选举信息

俄罗斯黑客论坛泄露了 1500 万佛罗里达州选民信息

澳大利亚天然气生产商的客户信息因漏洞而泄露

推特泄露了数百万用户的位置信息

2020 年有三万三千次的国家支持的钓鱼攻击

Gartner：明年全球数据中心基础设施指出将增长 6%

美国商务部等联合发布个人隐私保护白皮书

六家银行因侵害个人信息被罚逾 4000 万元

爱尔兰正在调查 Instagram 的儿童数据处理问题

此外，在数据安全技术与观点方面主要讨论了：

数字空间治理、物联网场景下的安全与隐私、个人信息保护法草案的解读（概述、从个人信息生命周期的角度）、隐私增强计算、数字孪生技术、“数字新基建”的安全态势、数字信任体系以及以数据为中心的安全模式。

全球动态

1. 六家银行因侵害个人信息被罚逾 4000 万元

10 月 21 日，中国人大网公布了《个人信息保护法(草案)》，同一天，多家银行因“侵害消费者金融信息安全”收到监管罚单。 央行公告显示，近日，央行相关分支机构依法对部分金融机构侵害消费者金融信息安全行为立案调查，分别对农业银行吉林市江北支行、中国银行石嘴山市分行、建设银行德阳分行、建设银行娄底分行、建设银行东营分行、建设银行建德支行及相关责任人予以警告并处以罚款。农行、中行、建行 3 家银行共 6 家分支行被罚超 4000 万。

https://www.secvery.com/3148.html

2. 在线游戏 Street Mobster 存在严重漏洞，190 万个用户信息造泄露

2020 年 10 月 22 日，研究人员发现大型在线游戏 Street Mobster 存在一个严重漏洞。该漏洞可能导致玩家用户名、电子邮件地址和密码以及存储在数据库中相关数据被破坏。

http://hackernews.cc/archives/32859

3. Gartner 称明年全球数据中心基础设施支出将增长 6%

2020 年 10 月 22 日，Gartner 发布了一份预测报告，预测该行业明年的全球支出将增长 6%。Gartner 表示，这一增长将得益于企业从冠状病毒大流行期间对其施加的现金流限制中反弹。它预计，到 2021 年，最终用户在全球数据中心基础设施产品上的支出将达到 2000 亿美元。

https://network.51cto.com/art/202010/629433.htm

4. 黑客声称已攻击了 50000 多台家用摄像设备，并在网上发布录像

2020 年 10 月 21 日，一个黑客团体声称已攻击 50,000 多个家用摄像设备，部分录像已在成人网站上发布，并声称支付 150 美元就可享受终身观看服务。已有 70 多名成员支付订阅费。部分被上传的录像显示来自新加坡。

http://hackernews.cc/archives/32766

5. 美国政府称俄罗斯 APT 团体入侵了其政府网络，可能窃取选举信息

2020 年 10 月 23 日报道，美国政府称俄罗斯政府资助的黑客组织已经瞄准并成功突破了美国政府的网络，并在网络安全基础设施安全局（CISA）和联邦调查局（FBI）发布的

一份联合安全建议中披露了这些黑客行为。该组织从 2020 年开始就一直瞄准美国数十个州和地方政府网络作为目标。

https://segmentfault.com/a/1190000037582827

6. 俄罗斯黑客论坛上泄露了 1500 万佛罗里达选民的数据

2020 年 10 月 22 日报道，一个活跃的俄罗斯黑客论坛泄露了大约 1500 万佛罗里达选民的数据。这次泄密发生在美国总统大选前两周，在俄罗斯黑客论坛上泄露的数据包含 14,973,822 条记录，包括佛罗里达州选民的姓名，选民 ID，电话号码，地址，出生日期，性别，种族，党派等。

https://cybernews.com/security/15-million-florida-voters-data-leaked-on-russian-hacking-forum/?web_view=true

7. 谷歌警告：2020 年有 33000 次国家支持的钓鱼攻击

Google 在 2020 年的前三个季度向其用户发送了 33,000 多个警报，以警告他们针对他们帐户的国家赞助的网络钓鱼攻击。

https://www.bleepingcomputer.com/news/security/google-warned-users-of-33-000-state-sponsored-attacks-in-2020/

8. 美国商务部等联合发布个人隐私保护白皮书

美国商务部、司法部和国家情报局联合发布个人隐私保护白皮书。主要内容是美国国家安全访问有关法律对个人隐私保护的规定，重点聚焦于欧盟法院在判决隐私盾协议失效（即 SchremsII）中提出的有关问题。

https://www.engage.hoganlovells.com/knowledgeservices/news/us-government-issues-white-paper-regarding-eu-us-personal-data-transfers

9. 爱尔兰 DPC 正在调查 Instagram 的儿童数据处理问题

2020 年 10 月 19 日，据外媒报道，爱尔兰数据保护委员会(DPC)是欧盟《通用数据保护条例(GDPR)》的监管机构，在 Instagram 对儿童个人数据的处理引发担忧后，该委员会对 Instagram 展开了调查。如果 Instagram 被发现存在违反隐私法的情况，拥有这家社交网络公司的 Facebook 可能会面临巨额罚款。

https://www.cnbeta.com/articles/tech/1042391.htm

10.澳大利亚天然气生产商 Kleenheat 客户名称和地址因系统漏洞而暴露

2020 年 10 月 19 日报道，澳大利亚天然气生产商

Kleenheat 已警告许多客户有关数据泄露的信息，这可能导致姓名和地址等信息被泄露。该公司在给客户的一封电子邮件中写道：“潜在的泄漏是 Kleenheat 最近在常规数据安全检查中发现的，并且并未在 Kleenheat 的内部系统中发生。”

https://www.zdnet.com/article/kleenheat-customer-names-and-addresses-exposed-in-system-breach/

11.Twitter 拥有的 SDK 泄漏了数百万用户的位置数据

2020 年 10 月 21 日报道，一系列使用 Twitter 拥有的过时代码的流行应用程序正在暴露其用户的位置数据。网络安全公司 Kaspersky 的研究人员发现，包括 MoPub 在内的多个 SDK 使用未经加密的数据的传输，多个应用程序在缺少数字保护的情况下发送敏感位置数据，总共这些应用程序已被下载近 1000 万次。

https://www.vice.com/en/article/k7ae9a/twitter-mopub-sdk-location-data?&web_view=true

业界观点

1. 主要国家数字空间治理实践及中国应对建议

从全球数字空间治理的主要做法来看，当前各国均将数字技术发展视为数字空间治理的优先方向，**重视通过数据跨境流动规则强化数据主权与安全，并对基于数据价值的经济利益分配与管理规则进行积极探索**。美欧数字空间治理能力与影响力在全球领先，中国有必要借鉴美欧经验，加强数字空间治理，提升影响力。

（1）加快核心技术研发与应用。

（2）进一步细化数据流动的规则条款和实施方案。

（3）加快完善国内数字经济治理规则。

（4）积极推动国际数字空间多边治理与共识。

https://www.secrss.com/articles/26489

2. 安全与隐私是未来物联网部署的最大挑战

物联网安全的发展远落后于物联网本身，国内外多份研究结果显示，企业采用物联网最大障碍来自对安全的顾虑。

(1) 识别是安全性的第一步。物联网设备不具备绝大多数传统的安全控制和发现工具。

(2) 物联网设备还可以充当网关访问内部和先前隔离的

网络。这种可见性的缺乏导致安全团队完全没有意识到这些设备所带来的风险。

(3) 在设计阶段还没有考虑到安全性。

(4) 许多物联网设备甚至没有为接收或运行软件更新进行配置，更不用说有些设备依靠电池运行，没有资源在上面运行安全控制。

未来的研究应该集中在确保每一个物联网设备都被统计和评估，确保硬件受到保护以及可以容纳软件更新。

https://mp.weixin.qq.com/s?__biz=MjM5MzMwMDU5NQ==&mid=2649144279&idx=4&sn=a317c906ae184a01452d3b44bd34039c&chksm=be8b32cb89fcbbdd9696c9736afcffc1c60bfe014b158dbfbcf003330f9a1c2e574640d25694&scene=27&k

3. 个人信息保护法草案如何捍卫个人信息安全

从内容上看，草案聚焦目前个人信息保护的突出问题，落实个人信息保护责任，加大违法行为惩处力度。

(1) 适用范围更加清晰。

(2) 职责分工更明确。

(3) 处理个人信息要先取得用户同意。

(4) 处理敏感信息限制更严格。

(5) 突发公共卫生事件中个人信息保护。

(6) 严格规范跨境个人信息提供规则。

(7) 强化个人信息保护责任和义务。

(8) 情节严重违法行为罚款金额高。

https://www.freebuf.com/articles/neopoints/252106.html

4. 详解个人信息保护法草案：从个人信息生命周期角度进行系统设计

草案共八章七十条内容，包括“个人信息处理一般规定”、“敏感个人信息的处理规则”、“个人信息跨境提供的规则”等专门章节。针对草案的亮点，可归纳为一个“内”和一个“外”。“内”是指草案以个人权利为核心理念，体现在草案的整个制度构造中，把知情同意原则作为一个主线。“外”则是指和过去零碎的、片段式的立法相比，草案对个人信息的整个生命周期进行了一个全流程的系统设计。从采集到使用，到安全保护、跨境提供，再到敏感个人信息的处理、管理部门的确定和法律责任，这是过去的几部立法都没有解决的问题。

https://www.secrss.com/articles/26438

5. Gartner 发布 2021 年重要战略科技趋势，隐私增强计算入选

2020 年 10 月 20 日，全球领先的信息技术研究和顾问公

司 Gartner 发布企业机构在 2021 年需要深挖的重要战略科技趋势。其中，隐私增强技术入选，Gartner 认为，到 2025 年将有一半的大型企业机构使用隐私增强计算在不受信任的环境和多方数据分析用例中处理数据。企业机构应在开始确认隐私增强计算候选对象时，评估要求个人数据转移、数据货币化、欺诈分析和其他高度敏感数据用例的数据处理活动。

https://www.secrss.com/articles/26373

6. 美军选择数字孪生技术解决数据安全问题

美国空军创新中心 AFWERX 近日选择了 Diveplane 公司的一项可创建敏感数据数字孪生的技术。该技术创造了一种可验证、保护隐私、与真实世界相匹配的合成孪生（synthetic twin）方法，在保护数据安全的前提下，加快数据利用和分析，用户选择的数据集可以在不干扰或损害原始数据的情况下被使用和分析。合成的等效数据集具有与原始数据相同的统计特性，但没有任何隐私、敏感或涉密信息。

https://www.secrss.com/articles/26326

7. “数字新基建”安全态势分析与技术应对

数据安全事件频发引发了全球各国对于数据安全与个

人信息保护的重视，新技术新业务的数据安全、隐私保护与公众安全的理性平衡、疫情期间的隐私安全底线、数据跨境流动和出口管制政策成为全球数据安全治理的主要焦点。后疫情时代，随着数字新基建加速推进，企业要通过不断提升数据安全技术能力来面对复杂多变的数据安全风险，把安全措施带到数据流通的每个环节。“零信任”“隐私计算”“联邦学习”助力企业打造覆盖数据全生命周期的安全能力体系。

https://mp.weixin.qq.com/s/7NHhAISIGKpx4cSr168MyQ

8. 数字经济时代新型数字信任体系构建

随着以“数字新基建、数据新要素、在线新经济”为核心特征的数字经济发展和智慧城市建设浪潮的全面来临，网络安全和数据安全已经成为当下经济社会发展的主要风险类型。但是，网络实体之间信任关系的普遍缺失，传统信任关系的难以为继和新型数字信任关系的持续缺位，已经成为制约数字经济和数字治理进一步高效发展的主要瓶颈。基于此，从传统信任理论模型出发，结合数字经济发展的特征及其发展过程中衍生出来的新型安全挑战，提出面向数字经济时代的新型数字信任概念及核心特征，总结分析其对数字经济发展和智慧城市建设的重大意义。

https://mp.weixin.qq.com/s/ckoZBgYqAuGDZx-vT7AaLw

9. 美国防部：以网络为中心向以数据为中心安全模式转变

2020 年 10 月 19 日，据外媒报道，美国国防部于 2020 年 10 月 8 日发布了首部《数据战略》，概述了打造“以数据为中心”的新型国防部所需的八项指导原则，四个基本能力和七大目标。其中，“数据安全”占据了七大目标中的最多篇幅。

纵观其战略，网络安全、数据安全在其中的分量不容小觑。随着数据应用领域越来越广泛，数据资源愈发成为国家主权和国家安全的重要组成部分。在数字时代背景下，国家的信息安全、数据安全愈发彰显着与传统军事、政治安全同等的分量。

https://mp.weixin.qq.com/s/odxcaU73cAqtprQ8bMI1uA