

全球数据安全观察

总第 27 期 2021 年第 3 期

(2020.01.11-2021.01.17)

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为[数据泄露](#)和[泄露数据买卖问题](#)。

1. [联合国泄露超过 10 万个环境署工作人员信息](#)
2. [辉瑞疫苗的被盗数据在线泄露](#)
3. [美国技术公司 Ubiquiti 发生数据泄露](#)
4. [Capcom: 39 万人可能受到勒索软件数据泄露的影响](#)
5. [数百万 Parler 用户数据被泄露](#)
6. [某公司拍卖个人信息被罚 320 万，买房包括平安惠普、拍拍贷等](#)
7. [黑客以 60 万美元出售 Windows 10 源代码](#)

此外，在数据安全技术与观点方面主要讨论了：

1. [金融行业是数据资产泄露的主要来源](#)
2. [2021 年数据产业的五大趋势](#)
3. [个人信息安全的保护措施](#)
4. [从生产要素角度看数据安全保护存在的问题](#)
5. [常见的数据安全风险场景](#)
6. [数据安全成为人工智能全面发展的重要制约问题](#)

全球动态

1. 联合国数据泄露暴露了超过 10 万个环境署工作人员记录

2021 年 1 月 17 日报道，研究人员已经揭露了一个安全漏洞，他们可以利用该漏洞访问联合国环境规划署(UNEP)超过 10 万名私人雇员的记录。数据泄露源于暴露的 Git 目录和凭证，这允许研究人员克隆 Git 存储库，并收集与超过 10 万名员工相关的大量个人信息(PII)。

<https://www.t00ls.net/articles-59400.html>

2. 辉瑞被盗新冠疫苗数据在线泄露

2021 年 1 月 13 日报道，欧洲药品管理局（EMA）近日透露，去年 12 月黑客从其服务器上盗取的某些辉瑞/BioNTech 新冠疫苗数据已在线泄漏。EMA 负责审查和批准 COVID-19 新冠疫苗，以及评估、监测和监督引入欧盟的任何新药。BleepingComputer 发现有不法分子在几个黑客论坛上泄露 EMA 数据。

<https://www.aqniu.com/industry/72434.html>

3. 美国技术公司 Ubiquiti 披露数据泄露

2021 年 1 月 11 日，美国物联网供应商 Ubiquiti 表示，

托管“某些”IT 系统的云提供商受到了黑客攻击，并建议客户在发现其托管在云中的 IT 系统之一遭到破坏后，更改密码并启用多因素身份验证。攻击者可以访问服务器，其中包含与 Web 门户 ui.com 的用户帐户有关的信息，公开的记录包括名称、电子邮件地址以及加盐和哈希的密码。

https://blog.csdn.net/weixin_45715145/article/details/11254465

6

4. **Capcom: 39 万人可能会受到勒索软件数据泄露的影响**

2021 年 1 月 12 日，Capcom 为他们的数据泄露调查发布了新的更新，并指出，多达 39 万人现在可能受到他们 11 月份勒索软件攻击的影响。在 12 日发布的调查的更新中，Capcom 表示，他们已经确认了 16415 个人的个人信息被泄露，受影响的人总数可能达到 39 万。

<https://www.bleepingcomputer.com/news/security/capcom-390-000-people-may-be-affected-by-ransomware-data-breach/>

5. **惨遭“开源”，数百万 Parler 用户数据全部泄露**

2021 年 1 月 12 日，据报道，黑客利用美国社交应用 Parler 的安全机制缺陷爬取了 99.9% 的用户数据，包括 100 多万条视频，并且已经开始建立在线档案，任何人都可查询。

<https://www.secrss.com/articles/28633>

6. 某公司卖个人信息被罚 320 万，买方包括平安普惠、拍拍贷等

2021 年 1 月 14 日报道，中国裁判文书网公布一份判决书——《北京智借网络科技有限公司、贤某某等侵犯公民个人信息罪一审刑事判决书》。判决书显示，上述公司在未取得受害人同意的情况下，向下游多家公司出售包含姓名、身份证号、手机号等个人信息，因犯侵犯公民个人信息罪，被处罚金三百二十万元。值得注意的是，买方涉及多家知名公司，如平安普惠、拍拍贷、你我贷等。

<https://www.secrss.com/articles/28709>

7. SolarWinds 事件持续发酵：黑客以 60 万美元出售 Windows 10 源代码

2021 年 1 月 13 日，据报道，在对 SolarWinds 事件的深入调查中，微软发现部分内部帐号被黑客获取，并访问了公司的部分源代码。而现在，有一名黑客以 60 万美元的价格出售 Windows 10 源代码，但是无法确定真实性。

<https://www.cnbeta.com/articles/tech/1077323.htm>

业界观点

1. 证券行业数据资产泄漏分析报告,金融行业是数据资产泄露的主要来源

数据资产泄露已经成为各行业安全问题的风险源头,近年来数据资产泄露事件逐年增多、危害范围不断增大。其中,证券行业数据历来都是黑灰产人员重点攻击的对象,是数据资产泄露的重灾区。根据权威媒体发布数据统计,近年来数据资产泄露风险态势愈发严峻,事件数量、影响人数和企业损失呈现逐年增长趋势。金融行业是数据资产泄露的主要来源,占到了42%,而数据资产泄露高发的互联网行业也只排名第二,占27%。出现这种情况是因为金融行业涉及到的人群大多是高净值人群,数据转化率高,变现能力强,黑灰产人员选择攻击的行业大多是金融行业,大部分购买数据的需求也集中在金融行业。哪里有利益,哪里就会有黑灰产人员的存在。

<https://www.anquanke.com/post/id/228538>

2. 2021年数据产业的5大趋势

由于远程工作模式的渐趋流行和数据泄露的增加,新冠疫情的全球大流行迫使企业全面加快其数字转型战略,并重

新考虑其数据安全方法。

- (1) 数据隐私和访问控制：品牌差异化推动收入增长
- (2) 在数据目录和元数据管理上的投资将会带来回报
- (3) 集成的混合数据平台将改变云应用的力量
- (4) 更垂直的数据分析和数据平台技术
- (5) 实施分布式数据管理模型的 CDO(担保债务凭证)

<http://www.hackdig.com/01/hack-250302.htm>

3. 全国 2020 年移动应用安全观测报告：个人信息安全保护措施

保护个人信息安全需要健全数据分级分类规则，完善网络数据安全立法。

确立网络数据安全分级分类的基本思路：场景差异会形成不同的正当价值和安全风险，分级分类保护应当成为网络数据安全立法的基本思路。

引导公共属性数据相互共享和对外开放：公共属性的数据也被称之为公共利益数据。公共属性数据的共享与开放包括企业对政务数据的使用、政府机构对企业数据的使用、政府不同部门之间的数据共享。

推动企业数据安全有序的利用与流转：企业数据是企业通过合法形式取得的具有完全权属、有限权属、无权属的各

类数据。对于完全权属和有限权属的数据，企业可以在权利范围内进行交易、共享和开放。

确保新技术对个人数据利用的安全：对于各类挖掘个人数据潜在价值的新技术，应当进行数据安全风险评估，并在相关法规中建立场景化的数据利用规则。

<https://www.anquanke.com/post/id/228457>

4. 从生产要素角度看数据安全保护存在的问题

数据通过动态流动创造价值、提高政府治理能力，同时也面临数据窃取、数据泄露、个人隐私安全等问题。为了保障作为生产要素的数据安全，需要正确理解认识数据特性，把握数据安全特点，建设以数据为中心的安全保障体系，切实保障数据参与生产过程各环节安全。

<https://www.secrss.com/articles/28656>

5. 常见的数据安全风险场景

内部场景：运维人员、开发人员、测试人员、数据分析人员的舞弊、滥用、操作失误、蓄意攻击等。

特权场景：数据滥用、操作失误、权限滥用、数据窃听等风险。

外部场景：黑客攻击、恶意爬取、SQL注入、数据泄露

等风险。

合规场景：GDPR/网络安全法/CCPA 等法律、行业监管、产品准入、数据跨境等风险。

第三方合作场景：数据合理性、权限滥用、API 接口攻击等风险。

<https://www.freebuf.com/articles/database/257969.html>

6. 数据安全成为人工智能全面新发展的重要制约问题

随着人工智能在产业和技术两个方面都在加快渡过“探索期”，逐步进入“成长期”，人工智能发展与数据安全将更加深度地交织在一起，数据安全问题已然成为人工智能突破关键转轨期所必须解决的重要制约瓶颈。

一方面，人工智能发展加剧了传统数据安全风险。在以“数字新基建、数据新要素、在线新经济”为重要特征的数字经济发展大背景下，人工智能的新发展必然伴随着数据总量的井喷式爆发，各类智能化数据采集终端的加快增长，数据在多种渠道和方式下的流动更加复杂，数据利用场景更加多样，整体数字空间对于人类现实社会各个领域的融合渗透更趋于深层，这将使得传统数据安全风险持续地扩大泛化。另一方面，人工智能催生了各种新型的数据安全风险。人工智能通过训练数据集构造和优化的算法模型，因其对于数据

资源特有的处理方式，将会带来数据污染、数据投毒、算法歧视等一系列的新型数据安全问题。

<https://mp.weixin.qq.com/s/Z1omjo63l4sndY7p1d21EA>