

全球数据安全观察

总第 40 期 2021 年第 16 期

(2021.04.19-2021.04.25)

摘要

安全事件..... 2

1. 西班牙 Phone House 感染 Babuk, 300 万客户的信息泄露.....2
2. 黑客免费泄露 2000 万个 BigBasket 用户记录.....2
3. 美国第二大汽车保险公司数据泄露.....2
4. 不安全的云存储导致能源供应商 Eversource Energy 数据泄露.....3
5. 苹果全球最大代工遭勒索: 窃取重要机密, 索要 3 亿赎金..... 3

政策形势..... 4

1. 数据安全法草案、个人信息保护法草案最新修改内容公布..... 4
2. 工信部: 将陆续出台 APP 个人信息保护相关规定和标准.....5
3. 推进“一带一路”数据跨境流动的中国方案..... 5
4. 央行发布《数据生命周期安全规范 》6

业界观点..... 8

1. 2020 年有多达 61% 的公司受到勒索软件的冲击..... 8
2. 中国与东盟开展数据跨境规则合作的现状与挑战..... 8
3. 国家工信安全中心: 《区块链与数据安全治理白皮书》 9
4. 超六成用户认为人脸识别技术存在滥用趋势..... 10

安全事件

1. 西班牙 Phone House 感染 Babuk, 300 万客户的信息泄露

2021 年 4 月 21 日，西班牙 Phone House 感染 Babuk，并被勒索 600 万美元（约 97 个比特币）的赎金。Babuk 在暗网称已窃取 Phone House 的 10 个数据库，其中包含了超过 300 万客户和员工的私人信息，例如姓名、出生日期、DNI、银行账户、个人手机、电子邮件、个人住所地址和工作公司等内容。

https://www.elconfidencial.com/tecnologia/2021-04-17/phone-house-ciberataque-chantaje-hackers-babuk_3038839/

2. 黑客免费泄露 2000 万个 BigBasket 用户记录

2021 年 4 月 25 日，威胁行动者在一个流行的黑客论坛上泄露了大约 2000 万个 BigBasket 用户记录，其中包含个人信息和哈希密码。

<https://www.bleepingcomputer.com/news/security/hacker-leaks-20-million-alleged-bigbasket-user-records-for-free/>

3. 美国第二大汽车保险公司数据泄露

2021 年 4 月 19 日，汽车保险供应商 Geico 数据泄露，

威胁参与者偷窃了保单持有人一个月以上的驾照，正在滥用在线销售门户网站，以获取保单持有人的驾驶执照号码。

<https://www.bleepingcomputer.com/news/security/geico-data-breach-exposed-customers-drivers-license-numbers/>

4. 不安全的云存储导致能源供应商 **Eversource Energy** 数据泄露

2021 年 4 月 20 日报道，新英格兰最大的能源供应商 Eversource 将客户的个人信息暴露在不安全的云服务器上之后，导致数据泄露。泄露的信息包括名称，地址，电话号码，社会保险号，服务地址和帐号。

<https://www.bleepingcomputer.com/news/security/eversource-energy-data-breach-caused-by-unsecured-cloud-storage/>

5. 苹果全球最大代工遭勒索：窃取重要机密，索要 3 亿赎金

2021 年 4 月 21 日报道，REvil 黑客组织公开宣称，入侵了著名笔记本代工厂广达电脑(Quanta Computer)，称窃取了苹果的设计蓝图，并且表示还将公布一些窃取的设计蓝图。索要 5000 万美元(约合人民币 3.25 亿元)赎金。

<https://mp.weixin.qq.com/s/8UarUvrXqlYeXwgKMo-3Sg>

政策形势

1. 数据安全法草案、个人信息保护法草案最新修改内容公布

2021年4月22日，全国人大常委会法制工作委员会举行记者会，发言人臧铁伟介绍立法工作有关情况并回答记者提问。

关于数据安全法草案（二次审议稿）拟作以下主要修改：一是，对草案中的数据安全等用语的含义予以完善。二是，完善数据分级分类和重要数据保护制度。三是，充实数据出境安全管理规定。

关于个人信息保护法草案（二次审议稿）拟作以下主要修改：一是，针对当前个人信息过度收集使用等突出问题，完善个人信息处理应遵循的原则。二是，完善、充实合法处理个人信息的情形、撤回同意、自动化决策、跨境提供个人信息等方面的规则。三是，增加死者个人信息保护的规定。四是，明确国家网信部门统筹推进个人信息保护工作的有关职责。五是，与民法典有关规定相衔接，完善侵害个人信息权益的民事法律责任。

<https://www.freebuf.com/news/270855.html>

2. 工信部：将陆续出台 APP 个人信息保护相关规定和标准

今年以来，工信部已累计完成 29 万款 APP 技术检测，对 1862 款违规 APP 提出整改要求，公开通报 319 款整改不到位 APP，组织下架 107 款拒不整改的 APP。

接下来，工信部将在充分征求意见基础上，会同相关部门发布《APP 个人信息保护管理暂行规定》，组织制定《APP 用户权益保护测评规范》和《APP 收集使用个人信息最小必要评估规范》等系列行业标准。

<https://mp.weixin.qq.com/s/7PwDprV8ps4RIi1Bw2G0GA>

3. 推进“一带一路”数据跨境流动的中国方案

目前，欧盟将自己的数据保护模式奉为圭臬，坚持要求其他国家向其看齐，方可与欧盟进行数据流动。美国则从政治经济利益出发，通过推行基于低水平保护的数据跨境流动模式实现数据向美国汇聚，在巩固和强化美国公司对全球数据掌控的同时，压缩了各国自主选择数据保护水平的规制空间。美欧划定数据流动“小圈子”的做法，并不符合中国倡导共建“一带一路”的指导精神。中国应当在尊重各国主权、安全、发展利益的前提下，通过双多边数据保护合作，切实促进基于“一带一路”的数据跨境流动，充分释放国际合作发展的潜力。

一方面，中国应当在签署共建“一带一路”合作文件时，纳入以 RCEP 数据跨境流动条款为蓝本的内容，从贸易规则层面锚定数据应能自由跨境流动的立场，并同时为各国维护各自主权、安全和发展利益留足空间。另一方面，中国应主动与“一带一路”共建国家开展双多边的数据保护专项合作，回应各自的诉求，缓解潜在的风险，尽可能地实现更大范围的数据能够安全有序流动，激发“一带一路”合作的潜力，最终实现“和平合作、开放包容、互学互鉴、互利共赢”。

<https://mp.weixin.qq.com/s/whXh2LYSFs6Nnlp46fH19w>

4. 央行发布《数据生命周期安全规范》

2021 年 4 月 8 日，《金融数据安全 数据生命周期安全规范》（JR/T 0223-2021）（以下简称《规范》）正式获批发布实施。《规范》由中国人民银行科技司发起，全国金融标准化技术委员会归口管理。

《规范》规定了金融数据生命周期安全原则、防护要求、组织保障要求以及信息系统运维保障要求，在具体内容上分为 9 个部分，并附有数据采集模式、数据传输模式、数据脱敏等四个附录。建立了覆盖数据采集、传输、存储、使用、删除及销毁过程的安全框架，适用于指导金融业机构开展电子数据安全防护工作，并为第三方测评机构开展数据安全检

查与评估工作提供参考。明确了金融数据进行采集、传输、使用、删除、销毁的整个过程中的详细要求。其中要求 App、Web 等客户端相关业务完成后不应留存三级及以上数据，并及时对缓存进行清理。还另外规定，三级及以上的数据内部传输，应采取数据加密、安全传输通道或安全传输协议进行数据传输。在原则上，三级及以上的数据不应对外传输，的确需要传输的，应经过事先审批授权，并采取技术措施确保数据保密性。

https://mp.weixin.qq.com/s/0pbTj76PHoHtOKKpT6M_tg

业界观点

1. 2020 年有多达 61% 的公司受到勒索软件的冲击

Mimecast 的最新电子邮件安全状况报告，基于对 1200 多名 IT 和网络安全从业人员的研究，显示企业在 2020 年面临前所未有的网络安全风险。勒索软件影响高达 61%，比去年的报告增加了 20%。

受勒索软件影响的公司平均损失了 6 个工作日的系统停机时间，37% 的公司表示停机时间持续了一周或更长时间。超过一半（52%）的勒索软件受害者支付了威胁者的赎金要求，但其中只有三分之二（66%）能够恢复其数据。剩下的三分之一（34%）尽管支付了赎金也没有看到他们的数据。

<https://www.cnbeta.com/articles/tech/1117529.htm>

2. 中国与东盟开展数据跨境规则合作的现状与挑战

随着 RCEP 的签订，“中国 + 东盟”有望成为全球最大的数字经济市场。与此同时，作为数字经济发展的基础性制度——数据跨境流动制度的建设，正成为双方戮力合作的新高地。

中国与东盟在数据跨境规则合作的现状主要表现在：第一，加强顶层设计，对接发展战略；第二，扩宽合作领域，

提升合作质量；第三，推动制度创新，加速数据合作。面临的主要挑战有：第一，多种数据规则同时存在，加剧了“制度过剩”的可能；第二，大国的地缘经济博弈加剧了东盟数据跨境规则形成中的复杂性；第三，“信任”依旧是摆在中国与东盟数据治理进程中的关键问题。

https://mp.weixin.qq.com/s/4pjILAocKqPCbyulr_mECw

3. 国家工信安全中心：《区块链与数据安全治理白皮书》

4月20日，区块链技术与数据安全工信部重点实验室发布《区块链与数据安全治理白皮书》（以下简称“白皮书”）。

白皮书针对国内外法律政策和技术标准，厘清了区块链与数据安全治理的制度和实践现状；围绕数据安全事件影响、危害程度、治理难度等方面分析了当前数据安全治理痛点；梳理了包括电力、政务、医疗、金融、汽车、征信、教育、中医药等领域在内的区块链数据安全治理应用场景；研究分析了区块链与数据安全存储、流通共享、安全审计、防篡改等数据安全治理环节的关联性，同时聚焦相关行业在数据安全治理工作中应用实际，初步提出了多种区块链技术的实现路径和应用方案。

https://mp.weixin.qq.com/s/43tfmnMvv-Uv_ExDrwe0zg

4. 超六成用户认为人脸识别技术存在滥用趋势

手机解锁、身份验证、上班打卡……人脸识别技术近年在人们生活和工作场景中大放异彩，与此同时，技术应用过程中涉及的用户隐私、信息保护问题也面临越来越大的挑战。2020年10月，全国信息安全标准化技术委员会等机构发布的《人脸识别应用公众调研报告（2020）》提出，有九成以上的受访者使用过人脸识别，其中超六成认为人脸识别技术存在滥用趋势，强迫使用、非法采集等问题多发。

https://mp.weixin.qq.com/s/QNIYVXEU_wM4wHXzKyU2mA