[公开]360NELab-DST-0-043-20210524

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 43 期 2021 年第 19 期

（2021.05.17-2021.05.23）

大数据协同安全技术国家工程实验室

目录

安全事件

1、23 款安卓应用程序泄露了超过 1 亿用户的个隐私数据

2021 年 5 月 21 日消息，Check Point 研究人员在分析报告中表示，约 1 亿用户的隐私数据遭泄露，原因是多个安卓应用中的错误配置，导致这些数据可能成为恶意行为者眼中的“肥肉”。这些问题源包括对实时数据库、推送通知和云存储密钥的错误配置，会导致电子邮件、电话号码、聊天信息、位置、密码、备份、浏览器历史记录和照片泄漏。

https://www.freebuf.com/articles/database/273878.html

2、TeamBMS 因 AWS S3 存储桶配置错误泄露 2 万多用户信息

2021 年 5 月 19 日， TeamBMS 因 AWS S3 存储桶配置错误泄露了 2 万多用户信息。该公司主要从事建筑管理系统领域的招聘工作，项目包括温布利球场、奥林匹克体育场和希思罗 5 号航站楼等。此次泄露了 21000 个文件，包括用户的电子邮件地址、全名、手机号码、家庭住址、社交网络 URL、出生日期、护照号码和申请人照片等。

https://www.infosecurity-magazine.com/news/recruiters-cloud-snafu-exposes/

3、印度航空遭受数据泄露，450 万客户受到影响

2021 年 5 月 22 日，在印度航空的乘客服务系统提供商 SITA 被黑客入侵两个月后，印度航空披露了一项数据泄露事件，影响了大约 450 万客户。暴露的客户详细信息包括姓名、出生日期、联系信息、护照信息、机票信息、星空联盟和印度航空的飞行常客数据以及信用卡数据。

https://securityaffairs.co/wordpress/118162/data-breach/air-india-data-breach.html

4、学生健康保险公司 Guard.me 遭受数据泄露

2021 年 5 月 17 日，学生健康保险公司 guard.me 在发现漏洞后，将其网站离线，该漏洞使威胁代理可以访问学生的生日、性别和加密密码，暴露了一些学生的地址、电子邮件和电话号码。

https://www.bleepingcomputer.com/news/security/student-health-insurance-carrier-guardme-suffers-a-data-breach/

5、冰岛因 InfoMentor 公司保护个人数据不力而处以罚款

2021 年 5 月 18 日报道，冰岛数据保护管理局已对 InfoMentor 公司处以 3500000 克朗(23100 欧元)的罚款，原因是该公司未能确保 Mentor 系统内的个人数据的适当安全，人

为错误是数据泄露的根源。Mentor 是一个为学校和其他与儿童相关的组织服务的信息系统，儿童的个人数据是此次受泄露影响的数据主体。

https://mp.weixin.qq.com/s/5W-WKWVoxPoCkTEdfZMoQQ

政策形势

1、《广东省社会信用条例》6 月 1 日生效，禁止商家采集个人生物识别信息

据人民网消息，2021 年 6 月 1 日起，《广东省社会信用条例》（以下简称《条例》）将正式施行，明确禁止商家采集自然人的宗教信仰、血型、疾病、病史、生物识别信息。

大数据时代，社会信用信息关系着每一个人的切身利益。《条例》强调对个人信息安全的保护，在相关环节设置了一系列保障措施，禁止采集自然人的宗教信仰、基因、指纹、血型、疾病、病史信息以及法律、行政法规规定禁止采集的其他信息。

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

2、新加坡 PDPC 更新《数据保护执法指南》

近日，新加坡个人数据保护委员会（PDPC）发布《数据泄露管理通知指南》和《数据保护执法指南》最新修订版。其中，《数据保护执法指南》详细阐述了《个人数据保护法》（PDPA）中新引入的自愿承诺（Voluntary undertaking）条款，进一步明确了 PDPC 的调查程序、执法行动类型和处罚措施等关键内容。

https://mp.weixin.qq.com/s/-MEb_VCFyy_K_bERm8dR4A

3、拜登下令强制推行零信任架构

近日，美国总统拜登签发行政命令（EO），旨在采用“大胆的举措”提升美国政府网络安全现代化、软件供应链安全、事件检测和响应以及对威胁的整体抵御能力，命令强调了云服务中静态和传输中的多因素身份验证和数据加密等网络安全现代化的关键举措和最佳安全实践。

https://mp.weixin.qq.com/s/HiYkwoicMfC_mb25DHBoOA

4、国家网信办通报 105 款违法违规收集使用个人信息 App

近期，针对人民群众反映强烈的 App 非法获取、超范围收集、过度索权等侵害个人信息的现象，国家互联网信息办公室依据《中华人民共和国网络安全法》《App 违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等法律和有关规定，组织对短视频、浏览器、求职招聘等常见类型公众大量使用的部分 App 的个人信息收集使用情况进行了检测，并通报了抖音等 105 款违法违规收集使用个人信息情况的 App。

https://mp.weixin.qq.com/s/PTeAalLKDpqm_8FbGfNvzQ

5、杭州公交、蘑菇街等 34 款 APP 因侵害用户个人信息权益等被通报

浙江省通信管理局通报了 2021 年第四批侵害用户权益行为的 APP，存在“违规收集个人信息”、“超范围收集个人信息”、“APP 强制、频繁、过度索取权限”、“强制用户使用定向推送功能”等相关问题,并要求问题 APP 相关企业限期整改。

https://mp.weixin.qq.com/s/4k17rqYPFO1UKJZ48qPqnQ

业界观点

1、勒索软件升级，运营模式升级为“三重勒索”

自 2021 年初以来，随着 Microsoft Exchange 漏洞的披露，勒索软件攻击的攻击次数增加了 57%。据估计，**2020 年勒索软件在全球范围内为企业造成的损失约为 200 亿美元，这一数字比 2019 年高出近 75%**。

自 4 月以来，**CPR 的研究人员平均每周看到超过 1000 个组织受到勒索软件的影响。与 2020 年初相比，受勒索软件影响的组织数量惊人地增加了 102%**。

勒索软件的巨大成功与“双重勒索”的运营方式不无关系。2020 年，支付赎金平均增加了 171%达到 31 万美元。**而 2021 年攻击者对“双重勒索”进行了扩展，升级为“三重勒索”**，与受害者相关的第三方也可能会被攻击者盯上。

https://www.freebuf.com/articles/neopoints/273177.html

2、关于“十四五”期间“数字中国”建设方面的若干建议

（1）在数字基础设计建设上，首要任务是主导开发新一代的多元化融合网络环境，替代单一技术路线、单一治理模式的“大一统”网络空间发展格局。

（2）在全球数字贸易领域，应努力构建全球范围内的

外交互信，围绕数据业务的互联互通做文章，重点打造多元化的共享共治的网络空间新范式。

（3）以新内生经济增长的视角审视数字经济内涵与外延，将数据纳入生产投入要素，建立真正意义的数据驱动的创新发展模式。

（4）“实践为基”，结合我国社会经济高质量发展需要，以数字化为抓手，推进国家治理现代化。

https://mp.weixin.qq.com/s/5R4l_onq8OuCenc_iw_VRA

3、培育壮大数据产业势在必行

随着数据的要素价值日益凸显，以及数据与新一代信息技术、新一轮产业变革的耦合共振、互融互促，数据产业将发生一系列关键性变化，实现从量的积累到质的飞跃、从“点”上的突破到“面”上的升级，并对经济发展、社会进步、国家安全乃至全球治理等诸多方面产生重大而深远的影响。

需科学研判世界数字化发展大趋势与我国当前发展实际，深刻认识数据这一新生产要素以及数据产业的重要性，抓住机遇培育壮大数据产业。

https://mp.weixin.qq.com/s/YDxB2Z2l-1SBD-64-Wvx4A

4、《数据安全治理白皮书 3.0》发布

5 月 13 日，“第四届中国数据安全治理高峰论坛”在北京圆满召开，峰会期间发布《数据安全治理白皮书 3.0》。

2021 年《数据安全治理白皮书 3.0》着重针对以下内容进行了修订：

（1）新增针对“数据安全、信息安全、网络安全”及“数据安全治理、数据安全管理”等近似概念间联系与区别的解读；

（2）更新“政务云及金融、能源、教育、电信运营商及医疗”等行业数据安全治理实践案例；

（3）新增数据安全相关政策、法律和标准介绍；

（4）新增数据安全治理国内外相关理论与介绍；

（5）新增数据安全治理发展进程中的问题与展望；

（6）更新国内外重大数据安全事件汇总；

（7）更新数据安全关键技术——新增数据资产梳理、差分隐私、数据安全运维、数据水印和数据使用行为溯源、多层次数据保护等内容；

（8）新增数据安全新兴前沿技术：多方计算、联邦学习、数据安全虚拟化引擎、数据安全 SAAS 能力等内容...

https://mp.weixin.qq.com/s/OMcQIFw4fv-V5ZdzBSuqMQ

5、《全球跨境数据流动相关问题研究》报告发布

5 月 20 日，国家工信安全中心第十三场“工信安全智库”系列报告在线发布活动——“全球数字政策瞭望专题”成功举办。中心信息政策所发布了《全球跨境数据流动相关问题研究》洞察报告。报告指出，当前我国在跨境数据流动机制构建和实践层面进行了探索，但是总体上还面临一些亟待破解的难题。一是法律制度和相关规则亟需完善和系统化。二是数据分类分级体系尚不健全，导致自由贸易试验区推行数据跨境流动缺乏基础。三是数据出境管制办法缺乏灵活性，无法完全保障数据出境安全和效率。四是主要经济体执法数据调取有冲突，导致数据跨境流动实践出现困扰。

https://mp.weixin.qq.com/s/UggLP9fJwy_Re-Ypis6jFQ