[公开]360NELab-DST-0-042-20210517

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 42 期 2021 年第 18 期

（2021.05.10-2021.05.16）

大数据协同安全技术国家工程实验室

目录

安全事件

1、Babuk 团伙声称已窃取日本的 Yamabiko 0.5TB 数据

2021 年 5 月 11 日，Babuk 团伙声称已攻击日本公司 Yamabiko 并窃取了 0.5TB 数据。Yamabiko 的总部位于东京，在全球范围内销售电动工具、农业机械和户外动力设备，年收入超过十亿美元。此次泄露的信息包括文件系统、Solidworks 文件、员工个人数据、财务报告、测试图和电路原理图等。

https://www.infosecurity-magazine.com/news/japanese-manufacturer-yamabiko/

2、暴露的数据库泄露了 20 万名退伍军人的医疗记录

2021 年 5 月 11 日，一个退伍军人管理局的供应商在网上公开了一个不安全的数据库，其中包含了将近 20 万名美国退伍军人的病历，暴露的数据包括患者姓名、出生日期、医疗信息、联系信息、甚至医生信息和预约时间，所有这些都可以用于社会工程攻击。该数据可能已被勒索软件攻击者窃取。

https://threatpost.com/veterans-medical-records-ransomware/166025/

3、大华银行因其员工遭到诈骗泄露千余中国公民的信息

2021 年 5 月 8 日，新加坡大华银行（UOB）因其员工遭到诈骗泄露千余中国公民的信息。据悉，该员工被冒充为中国警方的骗局所欺骗，泄露了 1166 名中国公民的个人详细信息，包括客户的姓名、身份证、手机号码以及账户余额等。大华银行表示，并没有客户的银行帐号泄露，并且其 IT 系统仍然是安全的。目前，该员工已被停职，并正在协助警方对此事进行调查。

https://mothership.sg/2021/05/uob-employee-leak-customers-scam/

4、亚马逊商家“刷点评”数据库大规模泄漏

2021 年 5 月 11 日报道，SaftyDetective 的安全研究团队上周四发现了一个在线暴露的 ElasticSearch“刷点评”数据库，包含大量供应商与刷点评用户之间的消息记录。其中包含大约 20-25 万个用户和亚马逊供应商的记录，包括用户名、电子邮件地址、PayPal 地址以及与亚马逊个人资料页相关的社交媒体账户。

https://mp.weixin.qq.com/s/pLc8THNB6Oo6CIMqXMAo2w

5、违反 GDPR 向中国传输数据，挪威一公司将被重罚 500 万克朗

2021 年 5 月 10 日，挪威数据保护监管机构（Datatilsynet）发布公告称，因道路收费公司 Ferde 向位于中国的数据处理者非法传输机动车驾驶者的个人数据，该机构拟对该公司处以 5 百万挪威克朗（约合 392 万元人民币）的罚款。

https://mp.weixin.qq.com/s/-ULV4FcVEH2PLkGv7CZLRw

政策形势

1、区块链隐私计算首个国际标准提案获 ITU 立项

在四月底举办的 ITU-TSG16 全体会议上，由蚂蚁链与中国信通院联合发起的标准 H.DLT-TEE《基于 TEE 的分布式账本系统机密计算》（TEE based confidential computing on distributed ledger technology system）成功获得立项，成为全球首个区块链隐私计算国际标准。这标志着中国在区块链领域的隐私计算技术受到国际社会的高度认可。

https://mp.weixin.qq.com/s/r_khxZkiAA562Z3JxIryhg

2、广东试点首席数据官制度，推进公共数据开放应用

近日广东省政府办公厅印发《广东省首席数据官制度试

点工作方案》，**鼓励试点单位先行先试，强化跨部门、跨层级、跨领域统筹协同机制，为全面落实首席数据官制度积累可复制、可推广的经验做法。**

首席数据官的职责将侧重于统筹数据管理和融合创新，推进公共数据共享开放和开发利用；领导本行政区域内数据工作，对信息化建设及数据发展和保护工作中的重大事项进行决策，协调解决相关重大问题；组织制订数据治理工作的中长期发展规划及相关制度规范，推动公共数据与社会数据深度融合和应用场景创新。

https://mp.weixin.qq.com/s/LC_XpMPD47HKsifxMWBCCg

3、广东省人民政府关于加快数字化发展的意见

广东省政府近日印发《关于加快数字化发展的意见》，加快建设数字广东，着力提升数字化生产力，构建广东发展新优势。意见表示，提高数字化治理能力，健全数据安全保护机制，提升重要数据和个人信息安全保护能力，强化数据跨境流动安全管理；全面梳理数字化关键领域产业链供应链风险，建立健全产业链安全管理体系和工作流程，在重点领域建立“链长制”，确保产业链供应链安全稳定。

https://mp.weixin.qq.com/s/PV389-pQjUDPjtxF7MuByA

4、网信办：《汽车数据安全管理若干规定（征求意见稿）》公开征求意见

为加强个人信息和重要数据保护，规范汽车数据处理活动，根据《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同有关部门起草了《汽车数据安全管理若干规定（征求意见稿）》，现向社会公开征求意见。

这是我国首个汽车数据安全方面的管理规定，是中国构建智能网联汽车网络安全体系的重要一环。征求意见稿聚焦于国家安全和公共利益，将加强个人信息和重要数据保护，对数据全生命周期的安全管理进行了框架设计。

https://www.secrss.com/articles/31150

业界观点

1、51%的组织遭遇过经由第三方造成的数据泄露事件

Ponemon 研究所的一份题为“第三方远程访问安全的危机”的新报告发现，51%的组织经历过由第三方造成的数据泄露。调查结果显示，大部分企业没有采取必要的措施来减少第三方远程访问风险，并使其网络面临安全和不合规的风险。因此，44%的企业在过去 12 个月内经历了漏洞，其中 74%的企业表示是由于给予第三方过多的特权访问而造成的。

https://www.youxia.org/2021/05/55656.html

2、勒索软件团伙已在暗网上泄露了 2103 家公司数据

自 2019 年以来，勒索软件团伙已经从暗网泄露了 2103 家公司的数据。现代化勒索软件行动始于 2013 年，攻击者的方式主要是对企业数据进行加密，然后要求支付赎金来获得解密。不过自 2020 年年初以来，勒索软件行动开始进行一种新的战术，称为双重勒索（double-extortion）。一位被称为 DarkTracer 的暗网安全研究员一直在追踪 34 个勒索软件团伙的数据泄露网站，并告诉 BleepingComputer，他们现在已经泄露了 2103 个组织的数据。

https://www.cnbeta.com/articles/tech/1125779.html

3、网络钓鱼，勒索软件和 Web 应用程序攻击将在 2021 年主导数据泄露

根据 Verizon 商业数据违规调查报告，去年，Web 应用程序占所有数据泄露事件的 39%，其中网络钓鱼攻击跃升了 11%，勒索软件增长了 6%。 以下是 Verizon Business DBIR 中得出的总结：

（1）85%的违规涉及人为因素。

（2）61%的违规行为涉及凭据。

（3）勒索软件出现在10%的违规事件中，比上一年翻了一番。

（4）在事件和破坏中，受损的外部云资产比本地资产更常见。

https://www.zdnet.com/article/phishing-ransomware-web-app-attacks-dominate-data-breaches-in-2021-says-verizon-business-dbir/

4、规范引导数字平台健康发展是时代面临的新课题

当今数字化、网络化、智能化已经成为时代特征和发展趋势，数字化、网络化、智能化在极大促进经济和社会的发展，但与此同时，数字化发展也为民众生活带来了不容小觑的安全风险和挑战。

发展数字经济首先要准确把握数字平台的属性与定位。从数据与监管的角度来看，数字平台中的**数据需要科学的分类与管理**。从责任的角度来看，数字平台的责任界定应该更合理、明确。

https://mp.weixin.qq.com/s/9V6M-QH5YFM0HMPW6yPk2A

5、企业隐私保护工作的挑战和实践探索

在隐私保护工作中，大多数企业面临的首要挑战是监管

合规。了解监管要求后，企业需要摸索隐私保护体系建设。由于隐私保护工作涉及不同部门联动，容易让具体措施的推行迷失在低效沟通中。

企业管理者要主动应对各种隐私风险和问题，持续关注隐私监管和行业标准最新动态，并积极参与隐私管理实践和隐私科技的发展。此外，隐私保护能力也将作为企业影响力的关键因素，从用户隐私体验、科技透明度和市场信任感上为业务赋能，帮助企业在数字化浪潮中创出佳绩。

https://mp.weixin.qq.com/s/2eh0baLOmuxvOuXcuDHpMQ