[公开]360BEST-DST-0-004-20200803

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 4 期 2020 年第 4 期

（2020.7.27-2020.8.02）

大数据协同安全技术国家工程实验室

全球动态

1、超过 50 个知名组织的源代码在线泄漏

2020 年 7 月 27 日，存储库基础结构中的配置错误导致泄漏了来自技术，食品，零售，金融，制造和电子商务等不同领域的数十个主流，知名组织的源代码。受影响的公司名单很长，根据银行安全部的说法，大约有 50 个组织的源代码已公开。其中包括一些大组织：微软，联想，Adobe，摩托罗拉，高通，AMD，GE 设备，联发科，Roblox，迪斯尼，任天堂，华为，海思，强生控件等。

https://www.hackread.com/source-code-of-high-profile-companies-leaked/

2、黑客免费泄漏 18 家公司的 3.86 亿条用户记录

2020 年 7 月 28 日，黑客正在将盗取的数据库发布到一个黑客论坛，该数据库是他们从 18 家公司中窃取的超过 3.86 亿用户记录。自 7 月 21 日以来，一个名为 ShinyHunters 的数据泄露卖家已开始在一个以出售和共享被盗数据而闻名的黑客论坛上免费公开数据库。

https://www.bleepingcomputer.com/news/security/hacker-leaks-386-million-user-records-from-18-companies-for-free/

3、在全球范围内识别出 9,517 个不安全的数据库并拥有 100 亿条记录

2020 年 7 月 29 日，根据 NordPass 密码管理器的研究，总共有 9,517 个不安全的数据库产生了超过一百亿个记录（10,463,315,645 个），已在线暴露给公众，无需任何安全验证。这些数据库包含电子邮件，名称，密码和电话号码等详细信息，显示了 NordPass 与 Hackread.com 共享的报告。

https://www.hackread.com/9517-unsecured-databases-with-10-billion-records/

4、Cloudflare 数据泄漏致近 300 万个站点的真实 IP 地址暴露

2020 年 7 月 27 日，乌克兰国家网络安全协调中心声称 Cloudflare 发生了数据泄漏，导致将近 300 万个站点的真实 IP 地址暴露在黑暗的网络上。

https://www.hackread.com/cloudflare-data-leak-expose-ip-addresses-ukraine/

5、化妆品巨头雅芳泄漏 1900 万条数据记录

2020 年 7 月 30 日，据报道，全球化妆品巨头雅芳（Avon）最近因云服务器配置错误泄漏了 1900 万条记录，其中包括个人信息和技术日志。暴露的数据库包含有关客户和员工的个人身份信息（PII），包括全名、电话号码、生日、电子邮件和家庭住址以及 GPS 坐标。此外包括 40,000 多个安全令牌、OAuth 令牌、内部日志、账户设置和技术服务器信息。

https://www.aqniu.com/industry/68937.html

6、视频制作服务商 Promo.com 数据泄露

2020 年 7 月 29 日，据报道，视频制作服务商 Promo.com 确认，因第三方服务的数据安全漏洞导致用户数据泄露。据称此次数据泄露可能涉及 2210 万用户的信息，其中包含 260 万条带有密码的记录。

https://www.securityweek.com/video-creation-service-promocom-discloses-data-breach

业界观点

1、我国目前涉及数据安全的法律法规

（1）《中华人民共和国网络安全法》

（2）《中华人民共和国数据安全法（征求意见稿）》

（3）《个人信息保护法》

（4）《网络安全审查办法》

（5）《数据安全管理办法（征求意见稿）》

（6）《网络安全等级保护条例（征求意见稿）》

https://www.freebuf.com/articles/neopoints/245025.html

2、2020 上半年我国网络安全相关的法律法规及政策

2020 上半年我国的网络安全相关法律法规及政策已有如下：（1）《中华人民共和国密码法》（2）《国家政务信息化项目建设管理办法》（3）《2020 年教育信息化和网络安全工作要点》（4）《网络信息内容生态治理规定》（5）《网络安全审查办法》（6）GB/T 35273-2020《信息安全技术 个人信息安全规范》（7）《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》（8）《个人健康信息码》系列国家标准（9）《工业数据分类分级指南（试行）》（10）《中华人民共和国数据安全法（草案）》。

https://www.freebuf.com/articles/neopoints/245025.html

3、我国当前数据安全和个人信息保护国家标准

目前围绕数据安全和个人信息保护两个方向已发布 6 项国家标准，在研标准 10 项，研究项目 18 项。其中已发布的标准如下：

序号	标准号	标准名称
1	GB/T 35273-2020	《信息安全技术 个人信息安全规范》
2	GB/T 35274-2017	《信息安全技术 大数据服务安全能力要求》
3	GB/T 37973-2019	《信息安全技术 大数据安全管理指南》
4	GB/T 37988-2019	《信息安全技术 数据安全能力成熟度模型》
5	GB/T 37932-2019	《信息安全技术 数据交易服务安全要求》
6	GB/T 37964-2019	《信息安全技术 个人信息去标识化指南》

https://www.freebuf.com/articles/neopoints/245025.html

4、使用数据安全治理框架来平衡业务需求和风险

Gartner 的治理研究报告称，使用数据的机会呈指数增长，但业务和财务风险也呈指数增长。建议负责数据、隐私安全和风险管理的负责人应做好以下几点：

一是使用数据安全治理（DSG）框架确定优先级并解决需要缓解的一系列复杂的业务风险。

二是研究在整个数据管理生命周期中如何出现优先业务风险。

三是使用连续自适应风险和信任评估（CARTA）选择适当的安全策略规则和控制措施，以减轻关键业务风险。

四是每年都要检查数据安全策略规则，并且每当业务风险发生变化时，都要检查并找出任何差距或不一致之处。

https://www.gartner.com/document/3978381?ref=solrAll&refval=257146270

5、新基建主旋律下的数据安全保障

当今中国经济，最大的主旋律是新基建。新型基础设施建设主要包括 5G 基站建设、特高压、城际高速铁路和城市轨道交通、新能源汽车充电桩、大数据中心、人工智能、工业互联网七大领域，涉及诸多产业链。数据和网络安全是新基建的基础支撑。近年来，我国持续性受到 APT 攻击，勒索软件攻击、数据泄露、漏洞威胁频发等。新基建带来新业务的同时也带来全新的安全挑战。

https://www.freebuf.com/articles/database/240383.html

6、区块链密码技术与应用实践

根据密码应用架构，区块链密码应用规范分为密码应用层、密码功能层和密码设备层。从密码学角度看，区块链中的关键技术，如交易账本、共识算法、通信加密、智能合约等都属于区块链密码应用层，即密码技术在区块链基础功能中的应用。密码功能层是密码学的技术实现，包括密码算法，密码协议，数字证明和密钥管理。密码设备层是密码规范中最底层部分，与硬件关联性较高，为功能层提供密码基础服务，如随机数生成、时间戳、签名验签服务等。

http://www.infoobs.com/article/20200727/40924.html

7、抗量子计算加密标准将于 2022 年发布

美国国家标准技术研究所（NIST）近日宣布，三年多的抗量子加密算法第二轮评审已经结束，评委会对入围第二轮的 26 个提议方案进行了评判，最终确定为 15 项。量子计算机可以轻松解决许多以前难以解决的问题，并且尽管该技术仍处于起步阶段，但随着它的成熟，它将能够击败许多当前的密码系统。

https://www.aqniu.com/industry/68893.html

8、DSMM 之数据采集过程安全

数据采集安全是数据安全生命周期的第一个过程，是对数据来源安全的管理，这是整个 DSMM 能够落实好的基础阶段，所有的后续工作都是以此为基础。所以该阶段的重要性不言而喻。该过程包含四个过程域，分别为：数据分类分级、数据采集安全管理、数据源鉴别及记录、数据质量管理。

https://www.freebuf.com/articles/database/207702.html

9、从数据安全运营看数据安全

近几年互联网公司数据安全已从单兵作战逐步发展到团队作战，分工上也朝着精细化运营、风险模型建设、数据安全平台建设等细分方向专业化演进。安全运营包括风险管控能力：识别、治理、收敛，在过程中结合业务特征提炼真实的风险场景、及隐私要求通过技术手段实现对法律法规的遵从性；还有运营赋能业务： 关键数据支撑业务决策，影响业务在风险环节的资源投入以及基础工具、组件服务支持，安全能力左移（前置），降低业务安全上的成本。

https://www.freebuf.com/articles/database/238364.html