

全球数据安全观察

总第 1 期 2020 年第 1 期

(2020.7.6-2020.7.12)

全球动态

1、上海 2 家科技公司被曝数据泄露

2020 年 6 月 30 日，Cybernews 研究人员发现上海孝信网络的 2 个含有上百万用户数据的数据库存在安全问题。其中一个数据库属于孝信通公司，数据库中含有超过 34 万条的敏感信息记录。另外一个数据库属于上海延华智能科技，数据库含有 420 万条记录，包括员工健康监控数据、车辆相关的信息和设施信息等。

<https://www.4hou.com/posts/kDXJ>

2、黑客勒索 23000 个 MongoDB 数据库，不交钱就泄露数据

2020 年 7 月 7 日，据 ZDNet 报道，2.29 万在网上暴露的 MongoDB 数据库被黑客勒索。据悉，这名黑客利用一个自动化脚本扫描配置错误的 MongoDB 数据库，删除数据库中的内容，然后留下一条勒索信息，要求用户支付 0.015 比特币（相当于 140 美元）。

<https://www.infoq.cn/article/bEfWcpImF2kIb1hb4CkY>

3、能源巨头北美可再生能源确认被勒索攻击

2020 年 7 月 9 日，EDP 北美可再生能源公司(EDPR NA)

证实了勒索软件攻击影响了其母公司 EDP 的系统。攻击者要求 EDP Group 支付 1580 比特币（相当于 1000 万美元或 990 万欧元）的赎金，以购买解密器，并停止公布从该集团服务器上窃取的 10 TB 数据。

<https://mp.weixin.qq.com/s/OFhe4i2INwdEP4iAqlnX0Q>

4、超 150 亿账号密码遭泄露在暗网交易

2020 年 7 月 9 日消息，据安全公司研究人员称，超过 150 亿账户的用户名和密码在网上流通，这些账户包括网络管理员账户、银行账户和流媒体服务。

<https://www.chinaz.com/2020/0709/1155952.shtml>

5、美国联邦调查局指控：FXMSP 黑客组织出售数百家公司网络访问权限

2020 年 7 月 10 日，据外媒报道，美国检察官已起诉一名黑客，该黑客被起诉出售全球数百家组织和公司的网络后门访问权限，是企业网络犯罪的幕后黑手。美国司法部表示，至少有 300 个组织和公司已经是受害者，根据受害者的不同性质，出售价格从几千美元到十万美元不等。

<https://baijiahao.baidu.com/s?id=1671790715162064742&wfr=spider&for=pc>

业界观点

1、对《数据安全法的认识》：中国版的封阻法令

主要关注《数据安全法》第三十三条提出的境外执法机构调取我境内数据的相关要求。此前，类似的条款已经出现在《国际刑事司法协助法》第四条。这样的条款很大程度上是为了应对近年来美、欧在因执法目的跨境调取数据方面的激进措施。《数据安全法》第三十三条和《国际刑事司法协助法》第四条本质上属于针对外国长臂管辖的“封阻法令”（the blocking statutes）。

<https://www.secrss.com/articles/23812>

2、数据安全是 AI 发展的关键

数据安全问题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。当前我国乃至全球人工智能领域都处于高速发展且成长空间巨大的转型阶段，面对差异巨大、场景各异的人工智能技术应用背景，应当切实、具象性地构建数据安全防御体系，针对不同技术应用场景和需求场景，应当准确设立针对性、高适用性的技术功能模块体系。

http://sh.xinhuanet.com/2020-07/11/c_139205378.htm

3、639 起上市公司数据泄露，平均损失高达 1.16 亿美元

2020 年 7 月 7 日，调研机构 Audit Analytics 回顾了 2011 年以来的 639 起上市公司网络安全事件，发现每起网络数据泄露事件的平均损失高达 1.16 亿美元。遭遇数据泄露的公司中，几乎有一半（43%）选择隐瞒不报。

<https://www.secrss.com/articles/23670>

4、数据安全的实现需要隐私增强的安全技术

继续使用加密和数据屏蔽作为通用控件。在需求大于挑战（包括有限的解决方案可用性）的情况下，选择新兴技术。对于不需要真实数据执行业务功能或原始数据必须与第三方共享的用例，请使用字段级数据转换。请注意，共享详细而不是汇总的数据会带来额外的隐私风险。对于需要第三方处理数据并得出结论或见解（例如产生汇总结果的分析）的用例，请使用基于软件的安全计算。如果必须在不受信任的环境中使用真实数据，请使用软件和硬件技术。这些技术中的一种或多种的选择取决于用例的适用性以及硬件技术的平台支持。

<https://www.gartner.com/document/3975583?ref=solrAll&refval=255102238>

5、7 大勒索软件发展趋势：帮派联手，拍卖被盗数据

2020 年 7 月 15 日，勒索软件 7 大最新发展趋势：Maze 勒索软件团伙提供“数据泄露即服务”；新的勒索游戏：拍卖被盗数据；有针对性的勒索软件攻击仍在继续；医疗保健行业持续受击；更多免费的解密程序；未修复的漏洞被有心之人利用；团伙组织可能仍在企业网络中安营扎寨。

<https://www.4hou.com/posts/n8J7>

6、人工智能应用于敏感信息安全的 5 种方式

2020 年 2 月，据 security affairs 官网报道，研究人员发现人工智能技术对确保敏感信息安全来说是一种非常好的工具。人工智能应用于数据安全保护的几种方式为早期检测、预测和预防、加密、口令认证和保护以及多因子认证。

<https://securityaffairs.co/wordpress/98120/security/artificial-intelligence-secure-sensitive-information.html>