[公开]360BEST-DST-0-007-20200824

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 7 期 2020 年第 7 期

（2020.8.17-2020.8.23）

大数据协同安全技术国家工程实验室

全球动态

1、 加拿大税务局遭黑客攻击！至少 5500 人账户被盗

2020 年 8 月 18 日，据 CTV 报道，加拿大税局（CRA）最近两次遭到黑客攻击，加拿大纳税人至少 5,500 个各类帐户被盗用，纳税人电子邮件地址和直接存款信息也被暴露。

http://www.safebase.cn/article-261399-1.html

2、 南非出现重大数据泄露事故，多达 2400 万人的个人信息被窃取

2020 年 8 月 19 日，南非信用机构 Experian 出现重大数据泄露事故，该网站有多达 2400 万南非人和 793749 个商业实体的个人信息被一名涉嫌欺诈者窃取。违规行为已报告给当局，众多南非银行，Experian 和南非银行业风险信息中心（Sabric）正在合作，正在进行相关调查。

https://www.zdnet.com/article/experian-south-africa-discloses-data-breach-impacting-24-million-customers/

3、 AI 公司 Cense 泄漏 260 万敏感医疗记录数据

2020 年 8 月 18 日，纽约一家名为 Cense 的人工智能公司暴露了近 260 万条包含敏感和机密数据的病历。安全发现

的研究人员和联合创始人耶利米·福勒（Jeremiah Fowler）于7月7日发现了暴露的数据，称有可能公开威胁数百万生命和身份的风险。

https://www.hackread.com/ai-firm-exposes-sensitive-medical-data-online/

4、 世界上最大的图形资源网站 Freepik 披露数据泄露，影响 830 万用户

2020 年 8 月 22 日，Freepik，一个致力于提供高质量免费图片和设计图形的网站披露了一个重大的安全漏洞。官方通报称，在黑客使用 SQL 注入漏洞访问存储用户数据的数据库之后，安全漏洞就发生了。Freepik 表示，黑客获得了在 Freepik 和 Flaticon 网站注册的 830 万最老用户的用户名和密码。

https://www.zdnet.com/article/free-photos-graphics-site-freepik-discloses-data-breach-impacting-8-3m-users/

5、 美国特勤局被曝购买追踪软件以获取公民位置数据

据 Engadget 网 8 月 18 日消息，美国特勤局(USSS)曾在 2017 年向私营软件公司 Babel Street 购买了 Locate X 追踪软件为期一年的订阅，以获取在流行应用程序中收集的设备数

据。而在一般情况下，执法部门需要授权或法院命令才能访问这些数据。美国各界认为，执法机构使用 Locate X 软件的做法侵犯了公民隐私权。目前，参议员罗恩·怀登（已提出一份名为《第四修正案不是用来出售的》的新法案，以禁止执法机构越权获取公民隐私信息。

https://www.landiannews.com/archives/78671.html

6、 因大规模泄露客户数据，万豪集团面临数百万人起诉

2020 年 8 月 20 日，据路透社伦敦消息，全球最大的酒店运营商万豪国际酒店集团因大规模泄露客户数据而面临数百万名曾经的酒店客人在伦敦发起的集体诉讼。这些客人要求万豪集团赔偿他们因个人数据而遭受的损失。有报道说，从 2014 年到 2018 年，万豪集团全球数据库中超过 3 亿条客户记录（可能包括护照和信用卡详细信息）被泄露。此案是迄今最大的数据泄露事件之一 。

http://www.safebase.cn/article-261402-1.html

7、 全球最大的邮轮运营商 Carnival 遭勒索软件攻击

2020 年 8 月 17 日，邮轮运营商 Carnival 透露，他们的子品牌在 8 月 15 日遭受了勒索软件攻击，导致该品牌部分信息系统被加密、数据文件被窃取。

https://www.bleepingcomputer.com/news/security/worlds-largest-cruise-line-operator-carnival-hit-by-ransomware/

8、 Microsoft 在最新 Windows 10 版本中默认启用 TLS 1.3

2020 年 8 月 20 日，微软表示，从 Build 20170 开始的所有 Windows 10 版本中，默认情况下将启用 TLS 1.3，这是将 TLS 1.3 在 Windows 中进行广泛部署的开端。

https://www.bleepingcomputer.com/news/security/microsoft-enables-tls-13-by-default-in-latest-windows-10-builds/

9、 犹他大学遭受勒索软件攻击并支付了 45.7 万美元赎金

2020 年 8 月 20 日，据报道，犹他大学在 19 日遭受了勒索软件攻击，为了避免数据泄露，犹他大学已经支付了 45.7 万美元的赎金。

https://www.bleepingcomputer.com/news/security/university-of-utah-hit-by-ransomware-pays-457k-ransom/

业界观点

1、 2020 年全球医疗数据泄露平均成本高达 713 万美元

根据 IBM Security 的 2020 年数据泄露成本报告，2020 年全球医疗数据泄露平均成本高达 713 万美元，这比去年增长了 10%以上，去年的行业平均数据泄露成本为 645 万美元。报告的五个主要发现：

(1) 远程工作会带来泄露风险；

(2) 尽管决策权有限，但首席信息安全官 CISO 仍应对泄露负责；

(3) 大多数网络保险企业使用第三方索赔费用；

(4) 巨大的泄露成本以数百万级飙升；

(5) 与报告中研究的其他威胁行为体相比，源于民族、国家攻击的数据泄露成本最高。

https://securityaffairs.co/wordpress/106710/reports/2020-cost-of-a-data-breach-report.html

2、 大数据环境下密码技术展望

针对大数据环境下的密码技术，目前业内专家学者们已经对可搜索加密、安全多方计算和全同态加密技术进行了广泛及深入研究，并在电子投票、智能电网及区块链等不同领

域取得了一定进展，但是仍然存在效率问题。当前认为解决效率问题的核心是优化算法性能，对于特定场景的算法优化可以使其在相应的应用领域提高效率。大数据环境下在满足大数据 5V 特征的前提下进行算法优化，对于整个大数据的应用研究至关重要。国家标准有助于规范行业的发展，提高行业竞争力。因此，大数据环境下应完善国家相关标准，保证数据本身的安全和数据拥有者的隐私安全。

https://www.secrss.com/articles/24850

3、 《数据安全能力成熟度模型》实践指南

《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）简称 DSMM 将数据按照其生命周期分阶段采用不同的能力评估等级，分为数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全六个阶段。DSMM 从组织建设、制度流程、技术工具、人员能力四个安全能力维度的建设进行综合考量。DSMM 将数据安全成熟度划分成了 1-5 个等级，依次为非正式执行级、计划跟踪级、充分定义级、量化控制级、持续优化级，形成一个三维立体模型，全方面对数据安全进行能力建设。

https://www.secrss.com/articles/24902

4、 陈纯院士、冯登国院士论数据安全治理

中国工程院陈纯院士强调的是时序大数据实时智能处理技术及网络安全应用。其中的关键技术是，

(1) 面向复杂时序特征指标的增量计算

(2) 面向网络时序数据处理的动态时间窗口

(3) 网络事件序列识别技术（复杂网络处理 CEP）

(4) 动态网络关联图谱的实时分析计算

中国科学院冯登国院士强调的是大数据环境下隐私保护与风险管控技术。目前的主要热点是，

(1) 身份匿名保护与去匿名化技术

(2) 敏感信息隐私挖掘与防护技术

(3) 密文检索与密文计算技术

(4) 基于风险分析的访问控制技术

https://mp.weixin.qq.com/s/JWBAZfDPW1QIjrRdc5Yb3Q

5、 推动数字“一带一路”发展形成新模式

中国数字化领军企业在“一带一路”推动海外投资和合作项目实施过程中重点突出、合作成果广泛，在发展过程中逐步探索出了“多中心+赋能+分享”的企业全球化新模式。中国数字化企业充分发挥“赋能者”的角色，各国本土优秀企业则主要承担新产品与服务的市场导入，确保本土化特性。

双方的合作基于“共商、共建、共享”的原则，重点包括以下几个领域。

(1) 信息技术服务与通信设施为数字化发展提供支撑

(2) 跨境电子商务与数字金融服务成为推广数字经济的重要抓手

(3) 智能化成为推进数字“一带一路”升级的重点

(4) 产业融合加快数字经济转型

http://www.hackdig.com/08/hack-114014.htm

6、 人工智能：淘汰一切可以淘汰的“人的因素”，才是网络安全未来最大的商机。

根据 MarketsandMarkets 人工智能网络安全预测报告，到 2026 年，人工智能网络安全市场规模预计将从 2019 年的 88 亿美元增长到 382 亿美元，年复合增长率高达 23.3%。欺诈侦测、用户/机器行为分析、风险评分、入侵检测和恶意软件检测是现阶段人工智能安全技术商业化潜力最大的应用（收益高、复杂性低）。与此相对，网络犯罪分子们也经常使用人工智能技术“降维打击”现有的安全防御体系：

(1) AI/ML 数据中毒与破坏

(2) 虚假音频技术入侵商务电邮

(3) 人工智能恶意软件规避沙箱

(4) 生物特征识别的猫鼠游戏

https://www.aqniu.com/news-views/64811.html

7、 国家级 APT 组织攻击频繁，安全应急响应成救命稻草

新冠疫情期间，黑客组织趁火打劫，网络攻击活动激增。具有国家背景的黑客组织频繁攻击我国政府与医疗机构。网络攻击防不胜防，快速响应、最大程度降低数据泄露风险成为当前最迫切需求。目前，应急响应呈现两大趋势：

(1) 关口前移，应急响应小时化

(2) 加快人才培养、引入第三方力量

https://www.secrss.com/articles/18501

8、 DSMM 之数据处理安全

数据处理，顾名思义，就是对数据进行操作、加工、分析等过程，此阶段对数据接触的最深入，所以安全风险也比较大。数据处理安全过程就是为了解决数据处理过程中的安全问题，降低该阶段的安全风险，该过程包含四个过程域，分别为：数据脱敏、数据分析安全、数据正当使用、数据处理环境安全。

https://www.secrss.com/articles/18501