[公开]360NELab-DST-0-020-20201130

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 20 期 2020 年第 20 期

（2020.11.23-2020.11.29）

大数据协同安全技术国家工程实验室

摘要

本期全球数据安全观察搜集到的重要事件的主要类型为**数据泄露、勒索软件**和**数据合规问题**。

1. 数百名高管邮件账户被泄露
2. 泰国王妃的私照被泄露
3. peatix.com 平台泄露 420 万用户数据
4. 法国 IT 巨头 Sopra Steria 遭勒索软件攻击
5. 法国 Banijay 感染勒索软件，已向英国和荷兰报告
6. 物联网芯片制造商研华股份受到勒索软件攻击
7. 澳大利亚情报机构利用 COVID-19 接触者追踪应用收集民众数据
8. Facebook 滥用个人信息，韩国开 67 亿韩元罚单据
9. 欧盟委员会《欧洲数据治理条例》提案发布

此外，在数据安全技术与观点方面主要讨论了：

安全备份（应对勒索软件的重要措施之一）；数据安全市场；合规驱动下的数据安全技术；合规视角下的数据安全发展趋势；基于区块链的数字身份研究；人脸识别的相关法规；敏感数据分类分级；隐私保护和个人信息保护的法治化。

全球动态

1. 黑客在暗网出售数百名 C 级主管邮件帐户的密码

2020 年 11 月 27 日报道，黑客正在出售全球数百家公司的 C-level 高管的电子邮件账户密码，这些数据正在一个名为 Exploit.in 的俄语黑客封闭式地下论坛上出售。这些账户访问权的价格从 100 美元到 1500 美元不等，这取决于公司规模和用户的角色。

https://www.zdnet.com/article/a-hacker-is-selling-access-to-the-email-accounts-of-hundreds-of-c-level-executives/

2. 泰国王妃 1400 张私照遭外泄：都是 SD 卡惹的祸

2020 年 11 月 26 日外媒报道，一名英国记者近日在脸书上表示，他于今年 8 月收到了一张神秘的 SD 卡，其中包含泰国王妃诗妮娜的 1400 多张照片。目前为止，这些照片的泄露来源不明，神秘 SD 卡的主人也不得而知。

https://www.secvery.com/4207.html

3. peatix.com 平台泄露了 420 万用户数据

2020 年 11 月 24 日，黑客泄漏了在活动组织平台 Peatix 上注册的超过 420 万用户的数据 ，该网站目前位列 Internet

上 Alexa 最受欢迎的前 3500 个站点之列。泄漏的信息包括全名、用户名、电子邮件以及加盐和哈希密码。

https://www.zdnet.com/article/hacker-leaks-the-user-data-of-event-management-app-peatix/

4. 法国 IT 巨头 Sopra Steria 遭勒索软件攻击，损失或超 5000 万美元

2020 年 11 月 25 日，法国 IT 服务巨头 Sopra Steria 在一份正式声明中表示，10 月 Ryuk 勒索软件攻击将导致 4000 万至 5000 万欧元的损失。Sopra Steria 是一家欧洲信息技术公司，在 25 个国家/地区拥有 46000 名员工，提供各种 IT 服务，包括咨询、系统集成和软件开发。

https://www.bleepingcomputer.com/news/security/sopra-steria-expects-50-million-loss-after-ryuk-ransomware-attack/

5. 法国 Banijay 感染勒索软件，现已向英国和荷兰报告

2020 年 11 月 27 日报道，Banijay 公开确认了一场网络事件，法国跨国生产和分销公司 Banijay Group SAS 于本月初遭到 DoppelPaymer 勒索软件攻击，并在事件期间被勒索软件运营商窃取了敏感信息。该事件导致员工和商业敏感数据可能受到破坏。

https://www.bleepingcomputer.com/news/security/masterchef-big-brother-producer-hit-by-doppelpaymer-ransomware/

6. 物联网芯片制造商研华股份受到勒索软件攻击，被索要 1250 万美元赎金

2020 年 11 月 28 日，Conti 勒索软件团伙袭击了工业自动化和工业物联网芯片制造商研华股份（Advan Tech）的系统，要求支付 750 枚比特币的赎金以解密受影响的系统并停止泄漏被盗的公司数据。

https://www.bleepingcomputer.com/news/security/iiot-chip-maker-advantech-hit-by-ransomware-125-million-ransom/

7. 澳大利亚情报机构被发现利用 COVID-19 接触者追踪应用收集民众数据

2020 年 11 月 25 日报道，澳大利亚一个政府监察机构发现，该国情报机构在一个名叫 COVIDSafe 的接触者追踪应用中，“偶然 ”收集了民众数据。随后，澳大利亚政府负责监督政府间谍和窃听机构的情报监察长在周一公布报告中声称，该应用数据是在 “合法收集其他数据的过程中 ”被收集的。

https://www.cnbeta.com/articles/tech/1057769.htm

8. Facebook 滥用个人信息，韩国开出 67 亿韩元罚单据

2020 年 11 月 25 日报道，韩国个人信息保护委员会以脸书未经用户允许，滥用韩国用户个人信息为由，向脸书开出 67 亿韩元（约合 3978 万元人民币）的罚单，并向执法部门提起刑事诉讼。脸书的信息滥用行为从 2012 年开始持续六年，共涉及 330 万名韩国用户。不仅如此，脸书还通过提供不完整资料的方式妨碍调查。韩国个人信息保护委员会成立于今年 8 月，是负责保护个人信息的中央行政机构。

https://mp.weixin.qq.com/s/rFYHf3xMmBiuCpd5SrEw_A

9. 欧盟委员会《欧洲数据治理条例》（数据治理法案）提案发布

欧盟委员会于 2020 年 11 月 25 日公布《欧洲数据治理条例》（数据治理法案）提案，以促进各部门与欧盟成员国之间的数据共享。建立机制，促进那些不能作为开放数据提供的公共部门数据的再利用；采取措施以确保数据中介机构在欧洲共同数据空间内作为数据共享或汇集的值得信赖的组织者发挥作用，使公民和企业更容易为社会利益提供其数据；促进数据共享的措施，特别是使数据的跨部门和跨国界使用成为可能，并使正确的数据能够被用于正确的目的。

https://mp.weixin.qq.com/s/I_bnLCF02gd0Ye-Q_LYlIg

业界观点

1. 安全备份是应对勒索软件的重要措施

面对勒索软件的攻击，备份无疑是行之有效的缓解措施。定期备份数据的企业，当检测到勒索软件攻击时，就有机会能够快速恢复数据并将破坏降到最低。正因为良好的备份如此有效，所以如今勒索软件的攻击者已经把矛头对准了备份流程和工具。所以，作为遭遇数据加密勒索时最后的防线和控制方式，备份也同样需要保护。

（1） 使用额外副本和第三方工具补充 Windows 备份

（2） 隔离备份

（3） 在多个位置保存多个备份副本

（4） 测试你的备份

https://www.chainnews.com/articles/229481339109.htm

2. 数据安全市场步入快车道，2020 年或达 52.5 亿

计世资讯（CCW Research）近日发布《2019-2020 年中国数据安全市场现状与发展趋势研究报告》。报告中指出，由于大量传统企业在数字化技术的加持下，逐渐转型为其业务可记录、可识别、可优化的大数据企业，并力求通过对数据价值挖掘，实现对业务的升级驱动及对企业流程、制度的

再造。2018 年中国数据安全市场达到 29.7 亿元，增速 29.6%，而 2019 年增速进一步提升至 32.7%，规模达到 39.4 亿元水平。同时，预计 2020 年市场规模将达到 52.5 亿元水平。

https://mp.weixin.qq.com/s/RYYCmv45PFz4_rZCqZ356w

3. 合规驱动下的数据安全技术盘点

Gartner 发布的 2020 年隐私成熟度曲线，涵盖了 35 种数据安全相关技术，种类丰富且繁杂，分别处在创新触发期、期望顶峰期、幻想破灭期、稳步爬升期和生产成熟期五个阶段。其中超过 70%技术处在稳步爬升期，说明该领域创新技术活跃，有巨大的发展空间，具体如下表所示。

技术成熟度	数据安全相关技术
创新触发期	机密计算、数据安全治理（DSG）、同态加密（HE）、差分隐私（DP）、主体权利请求（SRR）、零知识证明（ZKP）、5G 安全、合成数据、区块链的数据安全
期望顶峰期	数据泄露响应、安全多方计算（SMPC）、同意与偏好管理（CPM）、去中心化实体、数字道德、文件分析、隐私影响评估（PIA）、数据分类
幻想破灭期	保留格式加密（FPE）、人格化、隐私设计（PbD）、PHI 个人医疗隐私同意管理、移动终端威胁防御、云数据保护网关、隐私管理工具

稳步爬升期	数据销毁（Data sanitization）、安全即时通讯、电子取证软件、IT 风险管理方案、云访问安全代理（ CASB）、动态脱敏（DDM）、云应用程序发现
生产成熟期	数据库审计与防护（DAP）、云安全评估、数据库加密

https://www.freebuf.com/fevents/255985.html

4. 合规视角下的数据安全发展趋势观察

在隐私法规的强有力推动下，国内外数据安全相关技术和产品得到快速发展，逐步形成以“合规遵循”为主的安全细分领域。据 2019 年 11 月 Gartner 的一份预测报告指出，预测在 2023 年之前全球 80%以上的企业将面临至少一项以隐私为重点的数据安全保护规定，并且在合规上的投入将突破 80 亿美元。由此可见，数据安全合规未来仍然有广阔的市场应用前景。合规视角下的数据安全发展趋势观察如下：（1）欧美 GDPR /CCPA 驱动，用户数据权利响应自动化等相关技术发展迅速；（2）合规基础产品、敏感数据识别、数据脱敏市场日趋成熟；（3）合规与数据利用业务场景紧密结合，隐私增强计算技术与应用不断涌现；（4）数据安全治理框架与技术方案百家争鸣。

https://www.freebuf.com/fevents/255985.html

5. 《基于区块链的数字身份研究报告（2020 年）》发布

区块链作为新型信息处理技术，在信任建立、价值表示和传递方面有不可取代的优势，为数字身份管理提供了分布式信任基础。白皮书聚焦基于区块链的数字身份和认证体系，利用区块链的去中心化、多方共识、公开透明、防篡改、可追溯等特征赋能数字身份认证体系。

https://www.4hou.com/posts/QvQ9

6. 美国对人脸识别技术的法律规制及启示

人脸识别技术在维护公共安全、打击犯罪行为等方面具有广泛应用，但同时使用该技术也存在着风险，包括侵犯隐私权、自由权等基本权利，技术被商业组织或政府部门滥用，因技术不成熟而导致歧视、偏见等问题。

基于对上述风险的担忧，目前美国对人脸识别技术应用采取谨慎态度，在相关规则尚未出台前，限制政府部门对该技术的使用。在联邦和州立法层面，已经有规制人脸识别技术的立法尝试。这些尝试对我国规范人脸识别技术使用是很好的借鉴。

https://mp.weixin.qq.com/s/UEX95Mz4SnuC_tE7ZGgLEw

7. 浅谈企业敏感数据分类分级发展现状及思考

数据分类分级作为数据安全的“桥头堡”，在数据安全治理过程中至关重要。为此我们需要把主要精力放在敏感数据的管控上，制定精细化的管控原则。根据不同数据级别，实现不同的安全防护，避免敏感数据泄露给公司造成重大损失。实际分类分级落地过程中以下几点关键处则尤为重要：

(1) 推进数据分类分级落地，要从制度建立着手

(2) 清楚企业数据资产状况，明白敏感数据分布

(3) 根据相关指引，科学地对数据进行分类分级

(4) 数据分类分级是方法，精细化管控是目的

(5) 周期对敏感数据扫描发现，防患于未然

https://www.freebuf.com/articles/database/254780.html

8. 强化隐私保护技术与标准工作，推进个人信息保护法治化进程

随着个人信息保护法等一系列法律法规的制定和出台，也将为我国数据安全与隐私保护技术的发展带来新机遇。

真正落实法律法规中的各项要求离不开关键技术的支撑，实现个人信息保护法草案中规定的各项要求同样也需要众多关键技术，比如，数据跨域管控技术、密码技术、隐私保护技术等。

为实现对个人信息的保护，首先，要建立一系列配套的技术规范与测评规范，建立并完善相关的测评制度；其次，要注重法律法规及标准的宣贯工作，更好地引导企业逐步提升技术，实现相关关键技术与系统的升级；最后，个人信息保护是全社会广泛关注的问题，实现个人信息保护不仅要有法律的保障，而且要有极强的个人意识，更要有技术的有效支撑，并不能简单地对现有技术“踩刹车”或者“一刀切”。https://www.secrss.com/articles/27374