[公开]360NELab-DST-0-014-20201019

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 14 期 2020 年第 14 期

（2020.10.12-2020.10.18）

摘要

本期全球数据安全观察搜集到的重要事件主要有多种原因造成的数据泄露；国家机密和个人隐私数据被有组织地窃取；因隐私数据管理不当而发生的罚款、中国个人信息保护法草案首次亮相以及美军以数据为中心的网络安全防护。

IRCTC 在暗网泄露 90 多万用户数据

勒索软件黑帮窃取了育碧和 Crytek 的内部数据

希腊电信公司遭黑客攻击数百万个电话数据被窃取

黑客入侵家庭摄像机，发布 3TB 敏感剪辑视频

科技公司 Intcomex 被黑，1TB 数据被盗

国家安全机关破获数百起台湾间谍情报机关窃密案件

泰州警方破获一起侵犯公民个人信息（800 多万条）案

数据泄露使英国航空被隐私监管机构罚款 2000 万英镑

《中华人民共和国个人信息保护法（草案）》首次亮相

美军网络安全：2020 年底国防部将提供零信任架构

此外，在数据安全技术与观点方面主要讨论了：

加密技术四大创新领域（量子密码、同态加密、差分隐私、区块链）；基于 GDPR 的数据控制者和处理者；Gartner 发布的 2020 十大安全项目；政务系统风险评估的关注点以及《个人信息保护法》的分析与见解。

全球动态

1. 美军网络安全：2020 年底国防部将提供零信任架构

美国海军中将、美国国防信息系统局（DISA）局长、联合部队总部国防部信息网络部（JFHD-DoDIN）司令南希·诺顿（Nancy Norton）表示：美国国防部打算在 2020 年底前发布初始零信任参考架构，以改善网络安全。

事实表明：零信任架构正在引领国防部下一代安全架构的发展，从“以网络为中心”转变到“以数据为中心”，从“允许所有”转变到“拒绝所有”，从“边界防护”转变到“零信任”。

https://www.secrss.com/articles/26337

2. IRCTC 在暗网泄露 90 多万用户数据

2020 年 10 月 18 日报道，印度铁路餐饮和旅游公司（IRCTC）为印度铁路提供在线售票系统。作为印度铁路公司的子公司，泄露了近 100 万个用户数据。该数据已由用户在十月十三日与暗网社区共享。谁都可以轻松下载此数据。

https://www.secvery.com/2803.html

3. 勒索软件黑帮声称获得了育碧和 Crytek 的内部数据

2020 年 10 月 16 日，勒索软件黑帮 Egregor 宣称获得了知名游戏公司育碧和 Crytek 的内部数据。Egregor 在其网站上声称获得了育碧即将在本月晚些时候发布的游戏《Watch Dogs: Legion》的源代码，但暂时无法验证其声明是否属实。为了成功勒索受害者，流行的勒索软件在加密数据的同时会窃取数据。

https://www.solidot.org/story?sid=65821

4. 泰州警方破获一起侵犯公民个人信息案，涉及 800 余万条数据

2020 年 10 月 16 日报道，经过 6 个多月的缜密侦查，泰州警方破获一起侵犯公民个人信息案，抓获犯罪嫌疑人 7 名，被售卖的公民个人信息达 800 多万条。

https://www.secrss.com/articles/26311

5. 希腊电信公司遭黑客攻击数百万个电话数据被窃取

2020 年 10 月 15 日，希腊最大电信公司 Cosmote 向媒体通报，该公司上个月发生了一起重大的数据泄露事件，数以百万计希腊民众的电话以及信息数据被窃取，其中甚至包括总理和政府高级官员的通信数据。

https://baijiahao.baidu.com/s?id=1680673852489986757&wfr=spider&for=pc

6. 数据泄露影响逾 40 万客户，英国航空被隐私监管机构罚款 2000 万英镑

2020 年 10 月 17 日，据央视财经报道，英国信息委员办公室开展的一项调查得出结论，英国航空曾在缺乏足够安全措施的情况下处理大量个人数据，违反了数据保护法。英国数据安全监管部门信息专员办公室对英国航空公司因 2018 年客户数据泄露事件罚款 2000 万英镑，约合人民币 1.7 亿元。

http://www.bianews.com/news/flash?id=72530

7. 黑客入侵家庭摄像机，发布 3TB 敏感剪辑视频

尽管安全摄像机在远程监控儿童、老人和宠物等方面起着至关重要的作用，但它们还是网络罪犯的目标。据 10 月 12 日报道，网络犯罪分子能够入侵数以千计的家庭互联网协议（IP）摄像机，记录实时素材，并将其上传到网站上。目前已经上传了价值 3 TB 的已录制剪辑，而且还出售给了相关方，或者作为终身访问提供了 150 美元的一次性订阅费。

https://www.hackread.com/3tb-clips-hacked-home-security-cameras-leaked/

8. 国家安全机关破获数百起台湾间谍情报机关窃密案件

近期，国家安全机关组织实施“迅雷-2020”专项行动，依法打击台湾间谍情报机关渗透破坏活动，破获数百起间谍窃密案件，抓获一批台湾间谍及运用人员，打掉台湾间谍情报机关针对祖国大陆布建的间谍情报网络，有效维护了国家安全和利益。

https://mp.weixin.qq.com/s/cBkvaXcXnbN-91QNDV1yAw

9. 科技公司 Intcomex 被黑，1TB 数据被盗

2020 年 10 月 13 日，科技产品供应商 Intcomex Corp 遭受了数据泄露，其大约 1 TB 的用户数据被发布在黑客论坛上。其中包括信用卡详细信息，护照号码，许可证扫描，个人身份信息，工资数据，财务文件，客户详细信息，员工信息等。

https://cybernews.com/security/miami-based-tech-company-suffers-massive-1tb-data-leak/

10.《中华人民共和国个人信息保护法（草案）》首次亮相

2020 年 10 月 13 日，备受关注的个人信息保护法草案提请十三届全国人大常委会第二十二次会议审议。草案共八章

七十条，从内容上看，草案明确了适用范围，健全了个人信息处理规则，与民法典有关规定衔接，规定了个人信息处理活动中个人的各项权利，对敏感个人信息给出定义，成为公民个体权利的延伸。草案将知情权、选择权留给用户，对违法行为的处罚及侵害个人信息权益的民事赔偿等作了规定，情节严重违法行为处罚可达五千万。

https://www.freebuf.com/video/252241.html

业界观点

1. 加密技术的四大创新领域

从数据安全层面来看，“谁拥有数据”以及“谁可以读取哪些数据”这两个问题尤为重要。在这一系列的问题当中，需要加密算法将所有的东西结合到一起。**加密算法几个创新领域可以概括为：量子加密、同态加密、差分隐私和区块链。**

http://www.hackdig.com/10/hack-167779.htm

2. GDPR 下数据控制者及数据处理者

将控制者的概念拆分为 5 个构成要件进行单独分析，其中较为重要的是判断参与方是否满足“决定”和“目的和方式”要件。明确判断共同数据控制者之间存在共同控制权的总体标准是，各参与方是否共同参与决定数据处理目的和方式，共同参与可以通过共同决策的形式或决策合并的形式。处理者独立于控制者，且按照控制者的指示进行数据处理的实体；虽然数据处理目的和方式由控制者决定，但处理者有一定的自由裁量权，可以决定数据处理的“非核心方式”。

https://mp.weixin.qq.com/s?__biz=MzIxODM0NDU4MQ==&mid=2247489722&idx=1&sn=c970b8de65292f3719af245f26fc32ab

3. Gartner 2020 年十大安全项目

(1) 远程员工安全防护，尤指**零信任网络访问（ZTNA）技术**；

(2) **基于风险的弱点管理**，重点是基于风险来对弱点分级；

(3) 基于平台方式的检测与响应，特指**扩展检测与响应（XDR）技术**；

(4) **云安全配置管理**；

(5) 简化云访问控制，特指**云访问安全代理（CASB）技术**；

(6) **基于 DMARC 协议的邮件安全防护**；

(7) **无口令认证**；

(8) **数据分类与保护**；

(9) **员工胜任力评估**；

(10) **安全风险评估自动化**。

在峰会上，发言人 Brain Reed 给出了几点综合性建议：如果你只能做一件事，那么把保障员工远程访问的安全放在首位；在选择项目的时候，不要仅仅关注削减风险的项目，也要考虑一定做些体现业务价值的安全项目。

https://www.secrss.com/articles/26342

4. 政务系统信息网络安全的风险评估

互联开放的网络，资源交流便捷的同时，信息泄漏的隐患在逐渐加剧。尤其是与民生息息相关的政务部门。政务作为国家组织的重要组成结构，对国家的发展具有导向作用，政务系统信息存储着大量的有效信息，关乎着人民的切身利益，一旦发生信息泄漏，对人民及国家安全性会造成一定程度的威胁。基于此，保证政务系统的正常运作，对政务系统进行安全风险评估，是非常必要且应给予高度重视的。对电子政务系统进行评估时主要考虑的有如下几方面：非法黑客入侵；计算机病毒威胁；内网系统本身的漏洞；内部人员泄密；用户安全意识淡薄；系统安全软件本身的威胁。

https://mp.weixin.qq.com/s?__biz=MzAxMjE3ODU3MQ==&mid=2650488912&idx=2&sn=7f8a1abda124b4cfa0c2296e1e31d3e5

5. 《个人信息保护法》亟待解决的十大议题

我国《个人信息保护法》有亟待解决的十大议题，具体如下：

（1）法律定位：数据领域的基本法；

（2）基本原则：数据权利保护与数据流动的平衡；

（3）个人信息的定义：概括抑或列举；

（4）数据权利：增加抑或限缩；

（5）同意规则：明示抑或默示；

（6）数据共享和交易：生死存亡；

（7）数据跨境：自由抑或限制；

（8）数据泄露：实体和程序；

（9）监管机构：独立抑或综合；

（10）法律责任：严格抑或宽松。

https://www.secrss.com/articles/26241