[公开]360NELab-DST-0-016-20201102

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 16 期 2020 年第 16 期

（2020.10.26-2020.11.01）

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可分为**数据泄露、勒索软件和黑客攻击**以及**因数据泄露或不合规而发生的罚款**等。

Fragomen 律师事务所数据泄露， Google 员工信息暴露

NitroPDF 文档大规模数据泄露，包含谷歌、苹果、微软

印度新冠疫苗制造商遭数据泄露，被迫其关闭部分工厂

安全公司 Gunnebo 遭黑客攻击导致大量敏感文件泄露

阿里旗下电商平台 Lazada 110 万账户信息被黑客入侵

美国布鲁克林和佛蒙特州多个医院感染勒索软件 Ryuk

DoppelPaymer 勒索团伙泄露佐治亚州选民个人信息

黑客攻破心理治疗公司 Vastaamo，公布数百人健康数据

欧洲能源巨头再遭勒索软件攻击，5TB 数据被盗

黑客从加密货币服务中窃取了 2400 万美元

安泰人寿泄露上万条个人信息，罚款 100 万美元

万豪三亿客人信息泄露被罚 1.6 亿，面临多项集体诉讼

此外，在数据安全技术与观点方面主要讨论了：

第三方 SDK 个人信息保护；全球数字化转型；磁盘加密；远程访问；企业合规；安全认证；数据交易；安全意识的重要性；隐私发展趋势和多重环境下的数据安全治理。

全球动态

1. Fragomen 律师事务所数据泄露， Google 员工信息暴露

2020 年 10 月 27 日，据报道，美国最著名的移民法律师事务所之一 Fragomen，Del Rey，Bernsen&Loewy，LLP 披露了一起数据泄露事件。在未经授权的第三方访问包含与 I-9 就业验证服务有关的个人信息的单个文件之后，此安全漏洞暴露了 Google 当前和前 Google 员工的个人信息。

https://www.wangan.com/articles/1265

2. 阿里旗下电商平台 Lazada 110 万账户信息被黑客入侵

2020 年 10 月 31 日，阿里巴巴旗下电商平台、新加坡电子商务公司 Lazada 称，其 110 万账号信息被黑客入侵。在这个拥有 570 万人口的国家，这显然是一次重大的黑客入侵事件。这些账号信息包括用户家庭住址和部分信用卡号码等。

https://www.cnbeta.com/articles/tech/1047381.htm

3. 安泰人寿泄露上万条个人信息，罚款 100 万美元

2020 年 10 月 30 日，美国安泰人寿保险公司（Aetna）向美国卫生与公众服务部（HHS）下属的民权办公室支付 100 万美金并采取整改措施，以补救其此前违反《健康保险可携

性和责任法案（HIPAA）》导致的损害后果。

https://www.secrss.com/articles/26649

4. 万豪三亿客人信息泄露终被罚 1.6 亿，面临多项集体诉讼

时隔两年，万豪国际酒店集团旗下喜达屋酒店 3.39 亿客人个人信息泄露事件暂时告一段落。当地时间 10 月 30 日，英国信息专员办公室（ICO）发布声明称，因未能保护客户个人数据安全，对万豪处以 1840 万英镑（约合人民币 1.6 亿元）罚款。本次处罚只针对万豪在欧盟《通用数据保护条例》（GDPR）生效后的违规行为。

https://www.secrss.com/articles/26673

5. 美国布鲁克林和佛蒙特州多个医院感染勒索软件 Ryuk

2020 年 10 月 29 日报道，布鲁克林 Wyckoff Heights 医疗中心和佛蒙特大学健康网络是 Ryuk 勒索软件的最新受害者，该勒索软件大肆袭击了美国的整个医疗行业。美国政府与医疗保健行业的利益相关者举行了紧急电话，以警告他们“对美国医院和医疗保健提供者的网络犯罪威胁日益增加且迫在眉睫”。

https://www.bleepingcomputer.com/news/security/brooklyn-and-vermont-hospitals-are-latest-ryuk-ransomware-victims/

6. 安全公司 Gunnebo 遭黑客攻击导致大量敏感文件泄露

2020 年 3 月，KrebsOnSecurity 通知瑞典安全巨头 Gunnebo Group，黑客已侵入其网络，并将访问权出售给专门部署勒索软件的犯罪集团。Gunnebo 在 8 月表示已成功阻止了勒索软件攻击，**但在本周发现入侵者在网上窃取并发布了成千上万份敏感文件**，包括客户银行保险库和监控系统的示意图。

https://krebsonsecurity.com/2020/10/security-blueprints-of-many-companies-leaked-in-hack-of-swedish-firm-gunnebo/

7. DoppelPaymer 勒索团伙泄露佐治亚州选民个人信息

2020 年 10 月 29 日报道，DoppelPaymer 勒索软件帮派公布了从乔治亚州霍尔县盗取的未加密数据。10 月 7 日，佐治亚州的霍尔县宣布他们遭受了勒索软件攻击，从而影响了他们的网络和电话系统。

https://www.bleepingcomputer.com/news/security/georgia-county-voter-information-leaked-by-ransomware-gang/

8. NitroPDF 文档大规模数据泄露，谷歌、苹果、微软全中招

2020 年 10 月 28 日，PDF 文档服务 Nitro PDF 被曝光发生大规模数据泄露，**受影响企业超过 1 万家**，其中不乏 Google、Apple、Microsoft、Chase 和 Citibank 等知名企业。

https://www.aqniu.com/threat-alert/70928.html

9. 黑客攻破芬兰心理治疗公司 Vastaamo 并公布数百人健康数据

2020 年 10 月 26 日，黑客利用 Vastaamo 公司系统中的漏洞，成功访问了该公司数千名客户的数据库。据悉，勒索者索要约 45 万欧元（比特币形式支付）以换取不公布数千人的临床和心理健康数据。由于该治疗公司拒绝接受黑客的要求，于是黑客在网上公布了包括未成年人在内的数百人的健康数据信息。

https://www.cnbeta.com/articles/tech/1045357.htm

10.欧洲能源巨头再遭勒索软件攻击，5TB 数据被盗

2020 年 10 月 27 日报道，跨国能源企业 Enel Group 日前遭遇今年以来的第二轮勒索软件攻击。勒索软件 Netwalker 运营团伙此次为解密密钥开出了 1400 万美元的价码，如若

不从，则威胁公开多达 5TB 的被盗数据。

https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/

11.黑客从加密货币服务“Harvest Finance'”中窃取了 2400 万美元

2020 年 10 月 26 日，黑客从分布式金融（DeFi）服务 Harvest Finance 中窃取价值约 2400 万美元的加密货币资产，该网站使用户投资加密货币然后通过价格变动获得收益。

https://www.zdnet.com/article/hacker-steals-24-million-from-cryptocurrency-service-harvest-finance/

12.印度新冠疫苗制造商遭数据泄露，被迫其关闭部分工厂

2020 年 10 月 28 日，据外媒报道，近日印度新冠疫苗制造商雷迪博士实验室遭受网络攻击，迫使其关闭在巴西，印度，俄罗斯，英国和美国的工厂。为应对安全漏洞，新冠疫苗制造商已隔离所有数据中心服务。

这次攻击很可能是网络间谍活动的结果，该网络间谍活动目的旨在窃取有关新冠疫苗的研发信息。目前尚不清楚这次攻击是由某个国家或网络犯罪团伙实施的。

https://mp.weixin.qq.com/s/Qa3zzEqu8wor1woZFIHD-A

业界观点

1. 第三方 SDK 个人信息保护合规趋势及要点

第三方 SDK 的安全漏洞及收集使用个人信息规则不明确等风险给 App 治理及个人信息保护构成较大的威胁。中央网信办、工业和信息化部、公安部、市场 监管总局四部门已将 SDK 合规治理纳入 2020 年 App 专项治理工作的重点。

SDK 带来的**个人信息安全风险**主要包括：（1）SDK 自身的安全漏洞；（2）未明示 SDK 收集使用的个人信息规则；（3）SDK 超过业务必要情况过度收集个人信息。那么对于 SDK **个人信息安全合规治理的重点**是：（1）个人信息收集使用规则的告知同意；（2）个人信息处理活动的审计监督。

https://www.secrss.com/articles/26664

2. IDC：2021 年全球数字化转型 10 大预测

作为全球顶尖的数字化转型(DX)市场研究公司，国际数据公司(IDC)今天发布了《IDC FutureScape :2021 年全球数字化转型预测》，具体预测如下：

(1) 快速的 DX 投资创造更多经济引力

(2) 数字组织结构和线路图逐渐成熟

(3) 数字管理系统成熟

(4) 数字平台和扩展生态系统的崛起

(5) 数字优先方法

(6) 商业模式再造

(7) 可持续性与数字化转型

(8) 数字化原生文化

(9) 加速数字体验

(10) 商业创新平台

https://www.secrss.com/articles/26635

3. 企业安全建设-磁盘加密

众所周知磁盘加密一定意义上能够很好的保护企业电脑的数据安全，不会因电脑的遗失，被窃，暴力抢夺而被有心人获取到电脑上的资料。但是在具体操作中需要注意以下几个方面：

(1) **加密前**：数据备份、整体规划排期、自动执行脚本

(2) **加密中**：需要对一些可能出现的问题做一些应急处理（如系统崩溃、员工忘记密码）

(3) **加密后**：要排查是否有人私自解锁了硬盘等

https://mp.weixin.qq.com/s?__biz=MzU1NTkzMTYxOQ==&mid=2247484471&idx=1&sn=bc9dcfee70598f6917a8e16d3c355c52

4. 企业如何对核心机密进行远程访问

当前形势下，VPN 服务器的使用量随着远程办公的增加而激增。一项研究结果显示，仅在 2020 年 3 月，VPN 服务器的使用量就增加了 124%。公司员工和第三方比以往任何时候都更加依赖 VPN。**零信任访问**（实现对特定关键系统（而非整个网络）的细粒度访问）、**生物多因素身份验证**、以及**即时服务开通**等技术的进步让企业能够同时实现安全性和可用性，无需付出昂贵的代价。凭借上述技术方法，结合特权会话隔离和管理，能让企业在某些情况下完全不依赖于 VPN，从而减少 IT 管理团队的相关运营负担。

https://mp.weixin.qq.com/s?__biz=MzU2MTQwMzMxNA==&mid=2247494835&idx=2&sn=9eefb28e6081a06d6d2d3d14b0a8c536

5. 企业安全合规成本平均高达 350 万美元

Telos 最近开展了一项企业合规成本调查，于 2020 年 7 月至 8 月间对 300 名 IT 安全专业人员进行了调查，结果显示，平均每家企业必须遵守 13 个不同的 IT 安全和/或隐私法规，并且每年在合规性活动上花费高达 350 万美元，同时合规性审核每季度需要 58 个工作日。随着越来越多的安全法规出

台，越来越多的组织将其关键系统、应用程序和基础架构迁移到云中，违规风险和相关影响也随之增加。

https://www.aqniu.com/industry/70695.html

6. 2020 年需要关注的七个新增/热门网络安全认证

2020 年网络市场和资本热度不减，但安全人才荒仍在持续，对于任何有志在网络安全行业发展的人才来说，进入新的安全领域或提升职业竞争力最有效的办法之一就是取得权威安全认证。2020 年七个最热门、最具潜力的新增网络安全认证为：**数据隐私解决方案工程师、认证新兴技术道德技师、Kubernetes 安全认证专家、医疗健康信息安全和隐私从业者、信息系统安全认证专家、认证信息隐私技术人员、网络安全应急响应员。**

https://www.aqniu.com/news-views/70932.html

7. “人脸”贱卖，数据交易应强调合法性和公开透明

据媒体报道，在某些网络交易平台上，只要花 2 元钱就能买到上千张人脸照片(5000 多张人脸照片标价还不到 10 元)。信息时代给了不法分子可乘之机，强化数据安全性保护迫在眉睫。

首先，要从信息获取的源头进行治理，落实三大原则，

分别是合法、正当和必要原则。其次，信息企业要从技术上提升数据安全保护能力。同时，规范数据信息交易市场至关重要。健全相关立法，强化监管部门职能是对数据信息合法性的重要保障。

http://www.xinhuanet.com/tech/2020-10/28/c_1126665604.htm

8. 以人为本，安全意识工作大有可为

根据 Verizon 发布的《2020 数据泄漏调查报告(DBIR)》显示，网络钓鱼、利用窃取的账号密码、员工误发送、员工误配置被列为数据泄漏的前四大威胁。不难发现，从近年来的攻击趋势来看，黑客也讲究成本效益，相比利用软硬件漏洞，黑客更倾向于从阻力最小的“人”下手，利用“人的漏洞”即人的行为错误发起攻击，以此绕过企业的层层安全技术防御手段。某种程度上，企业员工对网络安全的冷漠无知、疏忽大意、意识淡薄已成为网络犯罪分子发起网络攻击的“首选武器”。在每个业务流程和信息系统中，人是最基本但也是不可预测的因素。

当人为错误成为造成数据泄露的最普遍原因时，这意味着每一个人都必须承担起自己的相应责任。发挥全员的力量，建立“人力防火墙”，打造企业安全文化是上策。

https://mp.weixin.qq.com/s/Q0lh5OmR8ePVh31LT2E3Tg

9. 2021 年预测：在过渡的一年中，隐私变得势在必行

2021 年将是过渡的一年，社区、消费者和企业将迎来新的常态。与隐私相关的三种趋势将成为这一转变的基础：

(1) 越来越需要收集，处理和共享来自消费者和员工的敏感个人数据；

(2) 尽管经济不景气，但基于价值的消费者仍将越来越倾向于与道德企业进行互动并将其数据委托给道德企业；

(3) 数据隐私相关的监管和合规复杂性将进一步增加。

在这种情况下，Forrester 预测在 2021 年：

(1) 与员工隐私相关的法规和法律活动将增加 100%。

(2) 四分之一的集体管理组织将加大对技术的投资，以收集零党派数据。

(3) CCPA 2.0 将通过并刺激美国联邦隐私立法的引入。

https://www.zdnet.com/article/predictions-2021-privacy-becomes-an-imperative-in-a-year-of-transition/

10.多重环境下的数据安全治理

随着组织业务不断发展，数据利用率越来越高，从之前数据孤岛到数据整合，从关系型到非关系型，从简单报表到敏捷 BI，从原有单点利用到现有全部支撑，可见数据如何充

分利用已成为支撑组织发展战略不可缺少的板块。

建议从以下安全方面做好数据治理措施：

(1) 态势感知归一分析

(2) 大数据安全

(3) 数据库安全

(4) 其他安全

以数据安全态势感知为核心，部署数据安全检测节点和数据安全管控节点，建立数据安全治理的整体解决方案。

https://www.freebuf.com/articles/database/241004.html