[公开]360NELab-DST-0-030-20210208

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 30 期 2021 年第 6 期

（2020.02.01-2021.02.08）

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**数据安全政策问题**。

1. 华盛顿州 160 万的失业申请中得数据被泄露
2. 警察考试数据库暴露了 50 万印度公民的 PII
3. EscortReviews 社区数据泄露，数十万人受影响
4. 欧洲排球组织云资产泄露数百护照信息
5. 安全公司 Stormshield 披露数据泄露
6. 某公司支付了数百万美元赎金后再度被勒索
7. Sprite Spider 成为最具破坏性的勒索软件之一
8. 拜登：美国采取“紧急”措施改善网络安全
9. 巴西国家数据保护局发布安全战略

此外，在数据安全技术与观点方面主要讨论了：

1. 2020 年度欧盟 GDPR 经典执法案例盘点
2. 欧洲《2020-2024 年数据保护战略》亮点及启示
3. 数据新要素需要提升新技能和新素养
4. 2021 年各企业需加强对数据隐私的关注
5. 2020 年美国数据泄露事件减少 19%
6. 360 报告：手机诈骗人均损失过万
7. 基于数据运营安全的个人信息保护

全球动态

1. 华盛顿州 160 万的失业申请中得数据被泄露

2021 年 2 月 2 日，华盛顿州审计师办公室遭受了数据泄露，暴露了 160 万份就业索赔中的个人信息。泄露的信息可能包括申请者全名、社会安全码、驾照、银行账号等。SAO 指责 Accellion 的文件传输设备(FTA)服务存在软件漏洞，该服务允许组织与外部用户安全地共享敏感文件。

https://thehackernews.com/2021/02/data-breach-exposes-16-million-jobless.html

2. 警察考试数据库暴露了 50 万印度公民的 PII

2021 年 2 月 2 日，CloudSEK 在一个著名的数据库共享论坛上发现了一个帖子，该帖子包含 500,000 印度公民的个人可标识信息（PII）。整个泄漏的数据库包含约 50 万条记录。由于数据库包含敏感数据，即姓名、手机号码和个人识别信息，因此使受害者容易受到网络钓鱼，诈骗甚至身份盗窃的攻击。

https://securityaffairs.co/wordpress/114148/data-breach/police-exam-database-exposes-500k-indian-citizens-pii.html

3. EscortReviews 社区数据泄露，数十万人受影响

2021 年 2 月 3 日，一个提倡女性护送和对其服务进行评论的在线社区遭受了数据泄露。该数据库包含 472695 多个成员的注册信息，包括其显示名称、电子邮件地址、MD5 哈希密码、可选的 Skype 帐户名称、可选的生日和 IP 地址。

https://www.bleepingcomputer.com/news/security/female-escort-review-site-data-breach-affects-470-000-members/

4. 欧洲排球组织云资产泄露数百护照信息

2021 年 2 月 1 日，研究人员发现一个公共暴露的云资产中包含数百张护照和身份证件的图像，这些护照和身份证件来自世界各地的记者和排球运动员。这些敏感文档托管在任何人都可以公开访问的 Microsoft Azure Blob 存储共享上。

https://www.bleepingcomputer.com/news/security/exposed-azure-bucket-leaked-passports-ids-of-volleyball-reporters/

5. 安全公司 Stormshield 披露数据泄露

2021 年 2 月 4 日报道，法国政府主要的安全服务和网络安全设备提供商 Stormshield 于今日表示，威胁行为者获得了访问其客户支持门户之一的权限并窃取部分客户信息。攻击者设法窃取了 Stormshield 网络安全防火墙的部分源代码，该

产品经认证可在敏感的法国政府网络中使用。

https://www.zdnet.com/article/security-firm-stormshield-discloses-data-breach-theft-of-source-code/?&web_view=true

6. 某公司支付了数百万美元赎金后再度被勒索

2021 年 2 月 2 日，据外媒报道，一家未披露名称的公司因勒索软件攻击而成为受害者，并向网络犯罪分子支付了数百万美元以恢复其数据，而在两周后仍然未能检查攻击起因，使得该公司成为该勒索软件团伙的二次受害者。

https://www.zdnet.com/article/ransomware-this-is-the-first-thing-you-should-think-about-if-you-fall-victim-to-an-attack/

7. Sprite Spider 成为最具破坏性的勒索软件之一

2021 年 2 月 1 日报道，在最近的 SANS 网络威胁情报峰会上，两位网络安全主管提供了一种被他们称为 Sprite Spider 的新型勒索软件的详细信息。像许多其他勒索软件攻击者一样，自 2015 年以来，Sprite Spider 攻击背后的团伙在复杂性和破坏能力方面迅速增长。如今，Sprite Spider 将成为 2021 年最大的勒索软件之一，其威胁程度与 5 到 10 年前的高级持续性威胁者相当。

https://www.csoonline.com/article/3604599/sprite-spider-emergi

ng-as-one-of-the-most-destructive-ransomware-threat-actors.html#tk.rss_all

8. 拜登：美国采取“紧急”措施改善网络安全

近日，拜登政府表示其正在发起一项改善国家网络安全的“紧急倡议”，指出对俄罗斯和中国“恶意行动”的担忧。拜登政府重点推动国家防御现代化，以应对不断演变的新风险。此外，拜登还将超过 100 亿美元的网络安全和信息技术资金纳入其 1.9 万亿美元的 COVID-19 复苏提案中，该提案将美国的网络安全描述为“重大危机”。

https://mp.weixin.qq.com/s?__biz=MzI4MjA1MzkyNA==&mid=2655316833&idx=1&sn=d4473a33fb6c2fdf4816731e21fa3b19&chksm=f02f972ac7581e3c232690383cd1fc0b2776c31b740ef8f24cbc4cc7a873191755931 50f7446&scene=0&xt

9. 巴西国家数据保护局发布安全战略

2021 年 2 月 3 日，巴西国家数据保护局发布了未来两年计划实现的进步及其三个战略目标：加强个人数据保护文化；建立保护个人数据的监管环境；改善法律合规的条件。

https://www.bleepingcomputer.com/news/security/leading-crane-maker-palfinger-hit-in-global-cyberattack/

业界观点

1. 2020 年度欧盟 GDPR 经典执法案例盘点

根据公开信息，自欧盟 GDPR 实施两周年以来，欧盟当局对违反 GDPR 的罚款已超过 3.3 亿美元。2020 年 GDPR 的相关执法活动相对前一年有所增加，欧盟相关监管机构已公开了 300 多起罚款，处罚事由主要集中在个人数据收集使用的合法性、员工数据保护、个人数据主体权利保障及数据控制者的安全保护义务等方面，同时考虑到疫情因素的影响及相关被处罚机构在个人数据保护方面的努力，部分监管机构降低了原有罚款金额。

https://mp.weixin.qq.com/s/cfYiBB6ozNxSDEEFt9WFQQ

2. 欧洲数据保护专员公署《2020-2024 年数据保护战略》亮点及启示

主要内容及亮点：关注现实问题—在疫情新常态下，必须解决防控带来的数据安全和隐私保护问题；坚持长远发展观—改变现有商业模式，推进数字经济转型和可持续发展；侧重个人信息权益保护—增强个人对自身信息的控制权，规制垄断供应商对数据的强制收集问题；呼吁欧盟一致行动—

在数据保护价值观、利益、目标、规则等方面达成协同；5.提前预防未来安全隐患—密切追踪和研究新技术引发的数据安全问题。**启示**：加强疫情常态化背景下对个人信息的保护；探索研究可持续的数字经济增长模式；增强数据安全执法力度和能力，形成有效威慑。

https://www.secrss.com/articles/29084

3. 数据新要素需要提升新技能和新素养

主要围绕理清数据新要素、构建新发展格局、提高治理新技能三方面。(1)数据是描述客观世界的手段，是自然世界投射到人脑中的镜像元素，而数字技术则是处理数据的高效工具，使现实世界、虚拟世界及生物世界构建映射关系成为可能。(2)数字化转型浪潮席卷全球，数字经济在国民经济比重持续提升。党的十九届五中全会特别提出，加快数字化发展，发展数据经济，推进数字产业化和产业数字化，推动数字经济和实体经济深度融合。(3)激活数据要素市场新活力，就需要从市场主体角度出发来设计激励机制，理清数据要素市场主体的权责关系，不断探索数据开放共享的新模式，进而培育一批优质大数据产业主体，构建良性的大数据产业生态体系。

https://mp.weixin.qq.com/s?__biz=MjM5MzMwMDU5NQ==&

mid=2649144933&idx=1&sn=9a581f329f7cea94059891ef3f91411e

4. 2021 年各企业需加强对数据隐私的关注

在 Spirion 2021 年客户数据隐私网络研讨会上，一组专家表示，今年企业必须更加关注数据隐私问题，因为这不再只是商业问题，而是个人问题。企业必须承认消费者拥有他们自己的数据，而企业只是在“借用”数据，这意味着企业在保护数据安全方面要格外小心。

https://mp.weixin.qq.com/s/JZAkzldEkgsx6i7Crnou7w

5. 2020 年美国数据泄露事件减少 19%

某家领先的非盈利机构称，2020 年美国公开报告的数据泄露事件减少 19%，原因在于攻击者从大规模窃取客户数据转向更有利可图的策略，如使用勒索软件。报告中共记录 1108 起网络安全事故，比 2019 年下降近 1/5，近 3.01 亿人受到影响，这一数据也比 2019 年下降 66%。进一步分析显示，在这 1108 起网络安全事故中，有 1001 次违规和 107 次数据泄露，这些数据往往是由云服务器的错误配置造成的。

https://mp.weixin.qq.com/s/NyJ3uhKbzLBRGBW-_AXdRw

6. 360 报告：手机诈骗人均损失过万，90 后成最惨“后浪”

近日，360 发布《2020 年中国手机安全状况报告》（以下简称“报告”）称，2020 年手机诈骗受害者人均损失 11345 元，90 成为主要受害群体。同时，与新冠疫情防控有关的诈骗内容正在成为不法分子的“新剧本”。

https://mp.weixin.qq.com/s/MAeP6DiRc3QhLKca5rlGGw

7. 基于数据运营安全的个人信息保护

个人信息因其自身携带隐私特性，与每个个体息息相关。个人信息保护不当，影响公众权益、企业利益以及社会秩序。在互联网、大数据、5G 万物互联的时代，个人信息被广泛收集和使用，必须妥善解决个人信息保护问题，才能保障整个数据产业健康发展。而现有的个人信息保护方法或技术，不足以应对新形势下的保护诉求。基于数据运营安全的个人信息保护，针对当前个人信息保护的新形势和新诉求，提出结合人工智能，通过数据运营安全对结构化、半结构化、非结构化的个人信息流动的保护，涵盖从生产到运维，从采集、传输、存储、处理、分析、共享、销毁全生命周期保护，深入数据运营中内嵌防护，同时与业务解耦， 达到保护个人信息安全的目标。

https://www.secrss.com/articles/29172