[公开]360NELab-DST-0-022-20201214

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 22 期 2020 年第 22 期

（2020.12.07-2020.12.14）

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. 美国顶级安全公司被 APT 组织攻击，红队工具被窃
2. 世界第三大飞机制造商的数据被黑客泄露
3. 酒店快递外卖成为信息泄露的重灾区
4. 欧洲药品管理局被攻击，目标为瑞辉新冠疫苗数据
5. 85000 个 MySQL 数据库在暗网出售
6. 富士康被黑客勒索攻击，索要 2.3 亿元赎金
7. 勒索软件迫使托管提供商 Netgain 关闭数据中心
8. 世界第三大飞机制造商被勒索软件“撕票”
9. 违规使用 cookie 存储个人信息，法国对谷歌、亚马逊开出亿元罚单

此外，在数据安全技术与观点方面主要讨论了：

ISO 29151 个人身份实践保护指南；零信任架构；APT 威胁趋势；勒索软件防御与响应；金融数据分类分级；数据加密趋势；数字“新基建”；数据安全解决方案（三位一体）；数据用益权。

全球动态

1. 美国顶级网络安全公司 FireEye 被 APT 组织攻击，红队工具被窃

2020 年 12 月 8 日，美国 FireEye 公司公开表示，一个拥有一流进攻能力的国家黑客组织窃取了该公司用来检测客户计算机网络漏洞的敏感工具，以寻求与政府客户有关的机密信息。事发后，《纽约时报》也发文报道，这次黑客攻击是 2016 年美国国家安全局（NSA）被攻击以来，最严重的网络安全工具被盗事件。

https://dy.163.com/article/FTE55LJ10511FSTO.html

2. 黑客泄露了世界第三大飞机制造商 Embraer 的数据

2020 年 12 月 8 日，据外媒报道，巴西航空工业公司被认为是继波音和空客之后的当今第三大飞机制造商，上个月遭到勒索软件的攻击。由于这家飞机制造商拒绝谈判，而是选择在不支付赎金的情况下，从备份系统中恢复了系统，参与入侵的黑客为了报复，泄露了该公司的一些私人文件，包括员工详细信息、商业合同、飞行模拟照片和源代码等样本。

https://www.zdnet.com/article/hackers-leak-data-from-embraer-worlds-third-largest-airplane-maker/

3. 北京三中院通报涉个人信息犯罪案件情况: 酒店快递外卖成信息泄露重灾区

2020 年 12 月 8 日报道，北京市第三中级法院于 12 月 4 日通报了该院审理涉公民个人信息犯罪案件的情况及典型案例。通过梳理这些案件，近几年被侵犯的公民个人信息数量从“倍数级”进阶至“指数级”爆炸式增长，酒店、快递公司、外卖平台等企业成为信息泄露的重灾区。

https://mp.weixin.qq.com/s/sAHWOelP50eZEzXktLzcaA

4. 欧洲药品管理局遭黑客攻击，涉及辉瑞新冠疫苗关键数据

2020 年 12 月 11 日据外媒报道，近日，负责批准新冠疫苗的欧盟监管机构欧洲药品管理局(EMA)表示，辉瑞公司提交的监管文件和 BioNTech 的新冠候选疫苗 BNT162b2 在攻击期间被非法获取。证实新冠疫苗研究可能是攻击的目标。

https://mp.weixin.qq.com/s/fMXqmaZg76TFRCrqD9ftug

5. 黑客在暗网出售超 85000 个 MySQL 数据库

2020 年 12 月 10 日，超过 85000 个 SQL 数据库目前在一个黑暗的 Web 门户上出售，价格只有 550 美元/数据库。黑客一直在窃取 MySQL 数据库，下载表格，删除原始

文档，并留下赎金记录，告诉服务器所有者与其联系以取回数据。

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

6. 富士康被黑客攻击，索要 2.3 亿元赎金

2020 年 12 月 9 日报道，富士康遭黑客勒索攻击，已加密约 1200 台服务器，窃取了 100GB 的未加密文件，并删除 20~30TB 的备份。消息人士还透露了勒索软件攻击期间在富士康服务器上创建的勒索信，内容如下所示。感恩节周末，富士康电子巨头在墨西哥的一家生产设施遭到了勒索软件攻击。攻击者在对设备加密之前先窃取了未经加密的文件。

https://nosec.org/home/detail/4618.html

7. 勒索软件迫使托管提供商 Netgain 关闭数据中心

2020 年 12 月 8 日，云托管和 IT 服务提供商 Netgain 在 11 月下旬遭受勒索软件攻击后，被迫将部分数据中心脱机。Netgain 为医疗保健和会计行业的公司提供托管和云 IT 解决方案，包括托管 IT 服务和桌面即服务环境。

https://www.bleepingcomputer.com/news/security/ransomware-forces-hosting-provider-netgain-to-take-down-data-centers/

8. 世界第三大飞机制造商 Embraer 被勒索软件“撕票”

2020 年 12 月 8 日，由于拒绝支付赎金，巴西航空工业公司（Embraer）被勒索软件团伙 RansomExx“撕票”——黑客将上个月在勒索软件攻击中窃取的 Embraer 公司的敏感数据泄露到了一个新的暗网站点上。据了解，上传在这个网站上的数据包括员工详细信息、商业合同、飞行模拟照片和源代码等样本。

https://www.aqniu.com/threat-alert/71622.html

9. 违规使用 cookie 存储个人信息，法国对谷歌、亚马逊开出亿元罚单

2020 年 12 月 10 日报道，法国国家信息与自由委员会（CNIL）发布公告称，由于谷歌及亚马逊法国网站此前存在违规使用 Cookie 的情况，该机构常委会于 7 日决定分别向谷歌和亚马逊两家公司开出 1 亿欧元（约合 8 亿元人民币）和 3500 万欧元（约合 2.8 亿元人民币）的罚单。

https://mp.weixin.qq.com/s/J4Zpgmmss9bKXe_BtBBcTg

业界观点

1. ISO 29151 个人身份实践保护指南

SO29151 全称是“ISO/IEC 29151:2017 个人身份实践保护指南”，是 ISO 标准委员会 2017 年颁布的指导组织实现隐私安全的一个国际标准，描述了个人可识别身份信息（PII）安全控制措施和风险处理指南。对于 ISO29151 标准本身来说，重点是标准第二部分附录 A，这部分是针对 PII 保护的特定控制措施，包含使用和保护 PII 的一般策略、同意和选择、目的合法性和指南、收集限制、数据最小化等 11 个隐私保护原则，共 27 个控制目标。

https://www.freebuf.com/articles/neopoints/250617.html

2. 构成“零信任生态系统”的 7 个主要元素

如今，企业的业务和商业流程已不再局限于物理环境内，传统以网络边界为中心的防火墙式安全防护机制已无法满足企业的发展要求，企业需要转向构建一个以数据和身份为中心的、与当下数字化发展趋势更加相适应的安全防护机制。因此，从 2018 年开始，Forrester 开始发布零信任拓展生态系统 Zero Trust eXtended (ZTX) 研究报告，并提出 7 个构成 ZTX 生态系统的主要元素，如下图所示:

https://www.freebuf.com/articles/security-management/247803.html

3. 2020 年 APT 威胁八大趋势

近日，卡巴斯基在其安全博客发布了 2020 年 APT 威胁全景图，并在 2020 年现状基础上，给出对 2021 年 APT 网络安全威胁的八大趋势预测：（1）APT 组织从网络罪犯那里购买初始网络访问权限；（2）越来越多的国家将法律起诉作为其网络战略的一部分；（3）更多硅谷公司将对零日漏洞经纪人采取行动；（4）针对网络设备的针对性攻击增加；（5） 5G 漏洞浮出水面；（6）勒索软件进化；（7）更具破坏性的攻击；（8）攻击者将继续利用 COVID-19 大流行。

https://www.aqniu.com/industry/71521.html

4. 勒索软件防御与响应的三大常见错误

2020 年，勒索软件已经成为很多企业的头号威胁，而 2021 年勒索软件将继续进化，攻击手段更加复杂，产业化程度不断提高，攻击范围也将扩大，更加难以防范。**三种常见的错误会导致预防不足和无效响应，并且各种规模的组织都犯了此类错误：**（1）无法从业务角度提出风险，这对于说服业务领导者提供适当的资金和政策支持至关重要；（2）在测试勒索软件准备情况方面不够深入；（3）DR（数据恢复）计划不足，无法解决可能感染备份的勒索软件威胁。

https://www.aqniu.com/news-views/71613.html

5. 《金融数据安全 数据安全分级指南》数据安全定级方式

数据分类分级是“保障数据依法有序自由流动”的重要基础，《金融数据安全 数据安全分级指南》作为金融标准中第一个“金融数据安全”标准，对通用数据分级工作具有较大借鉴价值。标准中明确数据定级原则主要为：合法合规性、可执行性、时效性、自主性、差异性、客观性。数据安全定级要素为数据安全性，主要依据影响对象、数据安全性遭到破坏后可能造成的影响程度确定数据安全级别。影响对象分为国家安全、公众权益、个人隐私、企业合法权益，影响程度分为严重损害、一般损害、轻微损害、无损害。最终将数据安全级别从高到低分为 5 级，其中 5 级涉及影响国家安全；4 级是普通金融机构最高级别数据；3 级以上在公众认知里即可识别为重要数据/敏感数据；2 级为企业机构内部办公常用数据；1 级为可公开数据。

https://mp.weixin.qq.com/s/D3-7JdRdn8Dv9-SQg_bzEw

6. 2021 年数据加密的六大趋势

(1) 云计算将扮演更重要的角色，尤其在金融服务领域；

(2) 同态加密将成为“新常态”；

(3) 自带加密（BYOE）将开始流行；

(4) 加密+密钥管理，对于缩短的证书生命周期至关重要；

(5) 加密技术对 DevSecOps 很重要，尤其是代码签名；

(6) 长周期设备制造商将开始拥抱加密敏捷性。

https://mp.weixin.qq.com/s/Mp0T1xtIQw2nWIF9xgNHiw

7. 夯实网络安全 助力数字“新基建”

各行业信息化建设的加速让网络安全产业得到蓬勃发展的新机遇，“新基建”加速建设也带来了各种网络安全新问题、新挑战。文章从以下四个方面概况了网络安全与“新基建”相互共生、相互依存的关系。

(1)“新基建”助力网络安全产业发展整体向好

(2)“新基建”加速网络安全细分市场成长

(3) 网络安全新技术助力“新基建”安全

(4)“新基建”浪潮下我国网络安全产业发展建议

https://mp.weixin.qq.com/s/xpPyaVjvrDHq-6GzS1XccA

8. 数据成基础战略资源，需建立三位一体数据安全解决方案

流动、共享和协同成为数据的新特征，数据跨系统、跨组织甚至跨境的流动和共享，协同计算，流动产生价值，数据是新时代的血液。数据安全问题重重，针对数据泄露、隐

私侵犯等问题，缺少真正有效的数据安全整体解决思路和方案。

建立三位一体的数据安全解决方案，包括以 DSMM 为抓手的数据安全治理体系，以安全大数据平台保障数据安全，以安全运营抵御持续变化的高级安全威胁。

https://mp.weixin.qq.com/s/ZEN5OhhO-xWBK_Ue5_PY1A

9. 论数据用益权

数据权属及其分配规则不清，已成为数字经济发展的最大制度障碍。未来应根据数据要素市场对数据积极利用的巨大需求，借助自物权—他物权和著作权—邻接权的权利分割思想，容纳作为现代新兴权利客体的数据。

https://mp.weixin.qq.com/s/uekGkF4gqjsEbfctBANjYA