[公开]360NELab-DST-0-024-20201228

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 24 期 2020 年第 24 期

（2020.12.21-2020.12.27）

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**和相关**数据法规条例发布**。

1. 英国能源公司客户数据库被泄露
2. NetGalley 的网站因黑客入侵而导致数据泄露
3. 耶路撒冷区政府网站因漏洞泄露居民信息
4. 加密钱包 Ledger 的 27 万用户信息被黑客泄露
5. Sangoma 被勒索软件 Conti 攻击导致数据泄露
6. 英国整容医院因勒索攻击导致 1TB 病人照片泄露
7. 《浙江省数字经济促进条列》发布

此外，在数据安全技术与观点方面主要讨论了：

1. 云计算安全防护
2. 自适应风险与信任评估的身份安全框架（CARTA）
3. 资产管理与运营
4. “零信任”安全体系实践原则
5. 同态数据加密环境商业化尝试
6. 2020 年重要的安全相关法律法规

全球动态

1. 英国能源公司数据遭泄露，整个客户数据库受损

2020 年 12 月 22 日，据报道，英国能源供应商 People's Energy 遭受数据泄露，影响了整个客户数据库。其客户的敏感个人信息，包括姓名、地址、出生日期、电话号码、电费和电表 ID 被黑客窃取。

https://mp.weixin.qq.com/s/tmA6Si_591UbVgjXkcO1fQ

2. NetGalley 的网站被黑客入侵后披露数据泄露

2020 年 12 月 24 日，NetGalley 图书促销网站遭受了数据泄露，使威胁行为者可以使用成员的个人信息访问数据库。泄露的数据包含 NetGalley 成员的个人信息，包括他们的登录名、密码、名称和电子邮件地址。NetGalley 是一个网站，允许作者和出版商向书籍拥护者、有影响力的读者和行业专业人士宣传其书籍的数字评论副本，以期将其推荐给读者。

https://www.bleepingcomputer.com/news/security/netgalley-discloses-data-breach-after-website-was-hacked/

3. 耶路撒冷区政府网站存在安全漏洞泄露居民的信息

2020 年 12 月 23 日报道，耶路撒冷区政府网站发现并修复了一个漏洞，该漏洞允许访问包含数十万居民个人信息的文件。该漏洞是由程序员 Hezkiyahu Raful 发现的，除了这个安全漏洞，Raful 还发现在 URL 中间更改数字可以访问建筑文件、票证、税务文件和“政府发布或接收的任何文件”。

https://www.jpost.com/israel-news/data-breach-discovered-in-jerusalem-municipality-website-653085

4. 黑客免费公布 27 万加密货币钱包 Ledger 用户信息

2020 年 12 月 22 日，一名网络攻击者在黑客论坛发帖，免费公布了从 Ledger 窃取的电子邮件和邮寄地址。一位威胁攻击者分享了一个存档，其中包括“All Emails (Subscription).txt” 和 “Ledger Orders (Buyers) only.txt”两个文本。All Emails (Subscription).txt 包含了 1,075,382 名订阅 Ledger 通讯的人的电子邮件地址; 而 Ledger Orders (Buyers) only.txt 包含了 272,853 名购买 Ledger 设备的人的姓名、邮寄地址和电话号码。

http://hackernews.cc/archives/34244

5. Sangoma 披露遭 Conti 勒索软件攻击及数据泄露事件

2020 年 12 月 24 日，在最近的 Conti 勒索软件攻击中文件被盗并在线发布之后，IP 语音硬件和软件提供商 Sangoma 披露了数据泄露。Conti 勒索软件帮派发布了从 Sangoma 窃取的超过 26 GB 的数据，这些泄漏的数据包括与公司会计、财务、收购、员工福利和薪水以及法律文件有关的文件。

https://www.bleepingcomputer.com/news/security/freepbx-developer-sangoma-hit-with-conti-ransomware-attack/

6. 英国大型整容医院遭勒索攻击，近 1TB 病人照片泄露

2020 年 12 月 25 日，据外媒报道，有黑客窃取了英国一家大型整容连锁店 Hospital Group 的数据并威胁要公布患者手术前后的照片和其他细节。Hospital Group 目前已经证实遭到了勒索软件的攻击。黑客组织声称已经获得了超过 900G 的病人照片。

https://mp.weixin.qq.com/s/Ql0Bf3TVtA_H7JZ8Qxy3cw

7. 《浙江省数字经济促进条例》发布

条例明确，发展数字经济是本省经济社会发展的重要战略，应当遵循优先发展、应用先导、数据驱动、创新引领、人才支撑、包容审慎以及保障数据安全、保护个人信息的原

则。条例所称数据资源，是指以电子化形式记录和保存的具备原始性、可机器读取、可供社会化再利用的数据集合，包括公共数据和非公共数据。公共数据，是指国家机关、法律法规规章授权的具有管理公共事务职能的组织在依法履行职责和提供公共服务过程中获取的数据资源，以及法律、法规规定纳入公共数据管理的其他数据资源。通过共享获得的公共数据，应当用于履行本机构职责，不得用于其他目的。

https://mp.weixin.qq.com/s/E-ROmyxLg_f-BRXEtcVbLg

业界观点

1. 云计算安全防护

云计算服务基于宽带网络特别是互联网提供，面临各类传统安全威胁，且安全问题随系统规模化而被放大。云计算系统中存放着海量的重要用户数据，对攻击者来说具有更大的诱惑力，如果攻击者通过某种方式成功攻击云系统，将会给云计算服务提供商和用户带来重大损失，因此，云计算的安全性面临着比以往更为严峻的考验。

开展云计算安全防护从以下几方面考虑：

（1）基础设施安全

（2）数据安全

（3）虚拟化安全

（4）身份认证与访问管理

（5）应用安全

https://www.freebuf.com/articles/security-management/256075.html

2. CARTA：数据分析驱动的身份安全

零信任架构主要针对的是安全防火墙基于网络拓扑的绝对信任的问题，规则引擎主要是利用人为既定的规则对访

问的安全进行一定程度的加固，而诸如图形验证码，条形验证码等技术为了防止机器人访问。Gartner 早在几年前就提出了 CARTA（Continuous Adaptive Risk and Trust Assessment）的概念，即连续自适应风险与信任评估的身份安全框架，这个框架当然是涵盖了零信任架构，但又不仅仅是零信任架构，主要还是突出连续，自适应与（量化）评估的属性。数据分析驱动的身份安全已经不再是纸上谈兵的理论阶段，如今随着相关技术与算法的成熟，身份安全领域实质已经进入了数据分析驱动的时代。随着更多的数据分析技术运用到身份安全领域之中，必然会带动符合 CARTA 标准的身份认证产品的诞生，从而使得整个行业的产品与功能更智能更人性化，满足人们对身份安全的差异化与个性化的需求。

https://www.freebuf.com/articles/security-management/252747.html

3. 企业安全建设的资产管理与运营

既然准备做资产管理，那第一步肯定需要目前企业资产的详细情况，因此我们可以从以下几个方面开始准备:

（1）梳理资产类型;

（2）与各类资产对接人，确认所需字段，统一各类资产表;

（3）收集已有资产数据;

（4）录入资产管理系统;

（5）确认各类资产变更流程;

（6）优化变更流程，实现自动化变更资产，保持资产实时更新。

已知资产梳理完成后，接下来肯定需要对未知资产进行管理，有资产发现和扫描结果处理。

最后是资产运营，资产最重要的还是全面性、准确性、实时性的问题，我们可以从以下几个方面去考虑:

（1）统一每类资产字段，避免各部门使用时存在纰漏;

（2）建议采用资产管理系统的方式进行存储与查询，有条件的单位可以创建 CMDB;

（3）嵌套入资产的变更流程中，包括新资产申请，下线，更换等方面，从源头控制;

（4）采用自动化的脚本或者程序去执行变更操作，人工审核或机器智能判断，保证实时性.

https://www.freebuf.com/articles/security-management/232452.html

4. “零信任”安全体系的实践原则

当数据构成我们的财富和核心竞争力时，传统的可信任

体系面临巨大挑战，无法满足用户数据安全的需求。我们需要构建零信任体系，以管理战略情报的思维来管理数据。其重要实践可总结为，

（1）从保护目标开始，知道保护什么才能谈得上安全

（2）保护要由内而外，不是由外而内

（3）以身份为基础而不是以账户为基础

（4）知白守黑，从正常行为和特征推断安全

（5）消除特权账户

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

5. IBM 发布企业同态数据加密环境，试水商业化

2020 年 12 月 22 日报道，IBM 日前发布了适用于企业的完全同态加密（FHE）测试服务，尝试将传输中加密数据分析引入商用。12 月 15 日，IBM 推出新版 FHE 解决方案 IBM Security Homomorphic Encryption Services（IBM Security 同态加密服务），称该服务可帮助客户开始实验如何实现 FHE 技术，从而更好地保护客户现有 IT 架构、产品和数据的隐私。

https://www.secrss.com/articles/28176

6. 2020 年国内受关注较高的安全相关法律法规

Top1: 《中华人民共和国个人信息保护法（草案）》

Top2: 《中华人民共和国数据安全法（草案）》

Top3: GB/T 35273-2020 《信息安全技术 个人信息安全规范》

Top4: GB/T 22240-2020 《信息安全技术 网络安全等级保护定级指南》

https://mp.weixin.qq.com/s/M8_tjvVYL_ImOfetbRm_og