[公开]360BEST-DST-0-008-20200831

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 8 期 2020 年第 8 期

（2020.8.24-2020.8.30）

大数据协同安全技术国家工程实验室

全球动态

1、中国禁止出口限制出口技术目录更新：涉及网络安全多项核心技术

2020 年 8 月 28 日，商务部、科技部对《中国禁止出口限制出口技术目录》（商务部 科技部令 2008 年第 12 号附件）内容作部分调整。其中有多条涉及网络安全技术：

1．新增密码安全技术（编号：186103X）

2．新增高性能检测技术（编号：186104X）

3．新增信息防御技术（编号：186105X）

4．新增信息对抗技术（编号：186106X）

5．新增基础软件安全增强技术（编号：186203X）

https://www.landiannews.com/archives/78671.html

2、SK 海力士 11TB 机密数据被黑客窃取，已有 5%被公开

据 2020 年 8 月 24 日韩媒报道，近期 SK 海力士遭受了黑客组织 Maze 的勒索攻击，目前 Maze 声称入侵了 SK 海力士 11TB 的数据，并公布了约 600MB 的数据信息，约占其总数据量的 5%。据悉，SK 海力士不是唯一遭受此黑客组织攻击的企业，LG 电子和佳能也遭受过 Maze 勒索软件的攻击。

https://www.t00ls.net/articles-57585.html

3、加拿大快递公司 Canpar Express 遭受勒索软件攻击

2020 年 8 月 24 日，据报道，加拿大快递公司 Canpar Express 成为了勒索软件攻击的目标，该勒索软件攻击影响了该公司某些系统。据路透社报道，由于勒索软件感染，Canuck 的网站下线了几天。据路透社报道，此事件对美国 Hat 居民产生了重大影响，包裹追踪和安排提货被阻止。

https://securityaffairs.co/wordpress/107476/cyber-crime/canpar-express-ransomware.html

4、来自伊朗的网络犯罪分子绿色袭击全球公司以牟取经济利益

2020 年 8 月 24 日报道，攻击者使用 Dharma 勒索软件和多种公共可用工具来针对俄罗斯、日本、中国和印度的公司。所有受影响的组织主机都具有面向 Internet 的 RDP 和较弱的凭据。黑客通常要求 1-5 BTC 之间的赎金。新近发现的黑客组织暗示，伊朗多年来一直是由国家资助的 APT 组织的摇篮，现在也可以容纳出于经济动机的网络犯罪分子。

https://securityaffairs.co/wordpress/107470/cyber-crime/cybercriminal-greeners-iran-attacks.html

5、830 万用户数据遭泄露！免费图片素材网站 Freepik 近日出现安全漏洞

2020 年 8 月 25 日讯，近日，Freepik 披露了一起重大安全漏洞，一名黑客(或多名黑客)利用 SQL 注入漏洞访问其存储用户数据的数据库，并获得了其 Freepik 和 Flaticon 网站上 830 万注册用户的用户名和密码。

https://www.sohu.com/a/414803828_100150040

6、多个社交 APP 数据被抓取，导致 2.35 亿用户数据泄露

2020 年 8 月 27 日，据外媒报道，Comparitech 的安全研究小组日前披露了一个不安全的数据库，导致 2. 35 亿 Instagram、TikTok 和 YouTube 用户的资料泄露到网上。

http://dy.163.com/article/FL1C1JG70511BI8B.html

业界观点

1、基于零信任打造封闭访问空间

零信任的理念和相关的技术正在快速推动网络安全行业的发展和变革，虽然所有的实名访问场景都可以逐步升级到零信任网络的安全框架下，但是在很长的时期内传统安全和零信任的混合状态会一直存在。尝试零信任的战略对任何一个企业而言，将是一个充满挑战的旅程，为了应对未来 5G 物联网时代复杂的网络攻击，必须要提前做好准备，**需要权衡封闭与开放、安全与便利的关系**，需要在保障应用访问安全的同时，给予用户最便利的访问方式，同时降低企业的管理和维护成本。

https://www.secrss.com/articles/25001

2、七成以上工控系统漏洞可远程利用

近日，Claroty 最新发布的工控系统安全报告发现，2020 年上半年披露的工业控制系统 （ICS）漏洞中，70%以上可以远程利用。报告详细介绍了国家漏洞数据库（NVD）发布的 365 个 ICS 漏洞和工业控制系统网络应急小组（ICS-CERT）在 2020 年上半年发布的 139 个 ICS 通报的评估，共影响到 53 家供应商。

https://www.aqniu.com/industry/69577.html

3、资产梳理和漏洞运营的挑战

在网络安全建设的过程中，资产梳理和漏洞运营作为其中的关键环节，常常遇到诸多挑战。

(1) 内部环境资产数量复杂难以梳理

(2) 内部环境资产管理难度大

(3) 缺乏应急能力

(4) 脆弱性排查难度高

https://www.aqniu.com/vendor/69578.html

4、民法典保护个人信息全生命周期的安全

2020 年 5 月 28 日，十三届全国人大三次会议表决通过了《中华人民共和国民法典》，自 2021 年 1 月 1 日起施行。该法律顺应互联网时代发展趋势，在网络安全、信息安全方面呈现诸多亮点。

(1) **守护个人安宁**。浓墨重彩保护公民隐私权和个人信息 。对隐私权作出清晰界定，全面治理广告电话、垃圾邮件、宾馆偷拍等侵犯隐私权社会顽疾。

(2) **构筑个人信息全生命周期保障体系**。强化对个人信息处理环节的规制。

https://www.freebuf.com/articles/database/239690.html

5、DLP 数据泄露检测原理浅析

根据 DLP 的实际用途，可将 DLP 检测分为 2 部分，**泄露关键字检测和近似重复文档检测**。

(1) **泄露关键字检索**。这一部分比较简单，在 DLP 后台配置一些敏感关键字或者正则表达式如 mobile 号、Bank card 号、ID 号等等。然后结合其他综合检测手法比如敏感词命中的次数、命中的频率、泄露的源等来判断是否存在泄露行为进而告警。

(2) **近似重复文档检测**。对获取到的从企业内部发送到企业外部的文档信息，需要检测这些信息中是否包含有企业机密文档库中的内容信息，如果判定是泄漏内容，需要对该信息进行拦截，避免产生泄漏事件。

http://www.hackdig.com/08/hack-114014.htm

6、数据要素：以数据安全保护为前提的新型生产要素

《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》正式公布（以下简称《意见》）。作为中央首份关于要素市场化配置的文件，《意见》分类提出了土地、劳动力、资本、技术、数据五个生产要素领域改革的

方向。**《意见》中明确强调了要做好数据开放共享的同时，推动完善适用于大数据环境下的数据分类分级安全保护制度。**加强数据安全管理的同时，又要鼓励数据合规应用。

数字化时代，数据一旦生产出来后就会进入传输、存储、处理、分析、访问与服务应用等各环节，任意一个环节都面临着数据安全挑战，造成数据失血。

因此，保护数据安全应以数据为中心构建防护策略，构建基于全生命周期的安全防护。

https://www.freebuf.com/articles/database/235061.html