[公开]360BEST-DST-0-011-20200921

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 11 期 2020 年第 11 期

（2020.9.14-2020.9.20）

大数据协同安全技术国家工程实验室

全球动态

1、错误配置的 Elasticsearch 服务器泄露 3.7 亿条记录的数据

2020 年 9 月 14 日，vpnMentor 发布了一份新报告，该报告调查了 70 多个网站的新数据泄漏，这些网站主要属于约会领域，也包括电子商务网站。

https://www.hackread.com/database-mess-up-leaks-ecommerce-dating-sites-data/

2、美国退伍军人事务部数据泄露影响了 46,000 名退伍军人

2020 年 9 月 15 日，美国退伍军人事务部周一发表声明称发生了网络安全漏洞，可能导致 46,000 名退伍军人的个人信息泄露，包括社会安全号码可能被泄露。

https://www.bleepingcomputer.com/news/security/us-dept-of-veterans-affairs-data-breach-affects-46-000-veterans/

3、我国 ZUC 序列密码算法作为国际标准 ISO/IEC 18033-4 补篇正式发布

我国 ZUC 序列密码算法作为 ISO/IEC 18033-4：2011/AMD1：2020《信息技术 安全技术 加密算法 第四部

分：序列密码 补篇 1：ZUC》已正式发布。ISO/IEC 18033-4：2011 规范了 MUGI、SNOW2.0、Rabbit、DECIMv2、KCipher-2 等序列密码算法，新发布的补篇 1 主要规范我国的 ZUC 序列密码算法。

https://dy.163.com/article/FMNKMMJV0534ECS5.html

4、2020 年上半年大型 DDoS 攻击上升 275%

根据 Neustar 的最新数据，与 2019 年上半年相比，2020 年上半年 DDoS 攻击的数量、规模大小和强度都有所增加，5 Gbps 或以下的小型 DDoS 攻击同比增长了 200%以上，而大型 DDoS 攻击（100 Gbps 及更高）显示了 275%的增长。

https://www.darkreading.com/threat-intelligence/ddos-attacks-rose-151--in-first-half-of-2020/d/d-id/1338937

5、巨型办公零售公司 Staples 披露数据泄露事件

2020 年 9 月 14 日，据报道，办公零售巨头 Staples 披露了数据泄露事件，威胁者未经授权访问了他们的订单数据。根据该公司发布的公告，没有敏感数据被泄露，未经授权的一方仅访问了 Staples.com 客户的有限数量的订单数据。暴露的订单数据包括客户的姓名，地址，电子邮件地址，电话号码，最后四个信用卡号码，产品成本，交货和订购的产品。

https://securityaffairs.co/wordpress/108271/data-breach/staples-data-breach.html

6、深圳振华数据库泄露，澳印媒体借机炒作

2020 年 9 月 15 日报道，深圳振华的一个数据库泄露，数据库包含大约 240 万人信息，绝大部分收集自社交网络。对此，澳大利亚堪培拉的网络安全咨询公司 Internet 2.0 表示：分析了其中 25 万人的记录，有 5.2 万美国人、3.5 万澳洲人和 1 万英国人，这些数据还包括了政客如英国首相 Boris Johnson，政客的亲戚、王室、名人和军人。振华泄露的数据库瞬间被炒作者利用，将其与政治挂钩。印度媒体也在同一天对此事进行了报告，并称深圳振华担负着“监控”1 万多名印度人的任务。

https://www.freebuf.com/news/249840.html

7、体验 iOS 14 的新数据泄露通知功能

2020 年 9 月 17 日报道，随着 iOS 14 的发布，Apple 引入了一项新功能，当用户存储的密码因数据泄露而受到破坏时，会向用户发出警告。

https://www.bleepingcomputer.com/news/apple/hands-on-with-ios-14s-new-data-breach-notification-feature/

8、LockBit 勒索软件启动数据泄露站点，双重威胁受害者

2020 年 9 月 16 日，据外媒报道，LockBit 勒索软件团伙在一个俄语黑客论坛上发布了一个指向其新数据泄漏站点的链接，将其用作其双重勒索策略的一部分，以恐吓受害者支付赎金。自 2019 年底以来，勒索软件团伙就采取了双重勒索策略，即在对网络中的计算机进行加密之前先窃取未加密的文件。然后，将被盗的文件以及它们将在数据泄漏站点上公开发布的威胁作为一种手段，诱使受害者支付赎金。

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-launches-data-leak-site-to-double-extort-victims/

业界观点

1、Gartner：2020 Top 8 安全与风险发展趋势

Gartner 分析师预测 2020 年安全与风险管理方面的 Top 8 发展趋势如下：

(1) 在主流市场上，XDR（扩展的检测和响应能力）成为 SIEM 和 SOAR 的备选方案；

(2) 安全流程自动化在逐步提高安全运维效率；

(3) 安全与风险管理负责人将承担起确保人工智能（AI）安全的职责；

(4) 网络对实体的影响造成了组织架构的变更，比如新增 CSO 岗位；

(5) 信任和安全团队开始保护消费者的数字化边界；

(6) 隐私正在日益成为一个有影响力的独立学科，影响着组织机构的方方面面；

(7) SASE 将传统 LAN 网络安全功能与 WAN 综合能力整合在一起，给网络安全带来重大变革；

(8) 云工作负载保护正在朝着新的、综合方向发展。

https://www.secrss.com/articles/25697

2、数据安全技术之数据脱敏

数据脱敏是指在不影响数据分析结果的准确性的前提下，对原始数据中的敏感字段进行处理，从而降低数据敏感度和减少个人隐私风险的技术措施。通常而言，数据脱敏分为三个阶段，首先，需要识别出数据库中的敏感字段信息；其次，采取替换、过滤、加密、遮蔽或者删除等技术手段将敏感属性脱敏，脱敏所使用的技术手段与下文提到的去标识化和匿名化用到的技术本质上没有不同；最后，需要对脱敏处理后的数据集进行评价，以确保其符合脱敏要求。总的来说，假名化、去标识化和匿名化都可以算是数据脱敏技术。

https://www.secrss.com/articles/25633

3、5G 时代下的网络数据安全治理

5G 网络是一个异构的网络，设备使用多种接入技术，各种接入技术对隐私信息的保护程度不同，各个数据安全泄露风险繁多。5G 作为国家新基建战略的首要基础设施，其安全性倍受国家及行业层面的重视，特别是 5G 网络引入的网络功能虚拟化、网络切片、边缘计算、网络能力开放等关键技术，一定程度上带来了新的安全威胁和风险。5G 数据安全防护应从以下几方面考虑：终端设备数据安全、无线接入数据安全、移动边缘计算数据安全风险、网络切片数据安

全、5G 业务数据安全。

https://www.aqniu.com/vendor/70080.html

4、97%的网络安全公司在暗网上泄漏了数据

全球应用安全公司 ImmuniWeb 在一份有关今年全球网络安全行业在暗网上暴露的最新报告中，发现 97%的领先网络安全公司的数据泄漏或其他安全事件都暴露在暗网上。平均而言，每个网络安全公司会暴露 4,000 多个被盗凭证和其他敏感数据，29%的被盗密码很弱，有 162 家公司的员工重用了他们的密码。正如 ImmuniWeb 的研究所示，即使是网络安全行业本身也无法幸免。

https://thehackernews.com/2020/09/dark-web-cybersecurity-report.html

5、2020 年 Gartner 十大安全项目发布

(1) Securing Your Remote Workforce（远程办公安全）

疫情让远程办公变成常态，通过 ZTNA 来保障远程办公安全。Gartner 认为采用 ZTNA 会驱动 VPN 替代。

(2) Risk-Based Vulnerability Management（基于风险的漏洞管理）

去年叫符合 CARTA 方法论的脆弱性管理，今年改叫基

于风险的脆弱性管理了。Gartner 认为补丁重要性是不同的，应该采用基于风险的方法来管理补丁程序，重点关注具有较高风险的系统和漏洞。

(3) Platform Approach to Detection and Response（检测与响应的平台方法）

去年叫 Detection and response，今年多了个平台化。把众多安全设备检测数据集中包括 EDR、SWG、CASB、IAM、DLP、NGFW 等。然后做数据规范化后，形成数据湖，分析数据相关性，最后通过事件响应、自动化、工作流和 APIs 实现响应。总结一下就是拓展检测数据源，提升数据分析能力，最后落实到自动化响应上，这个貌似没什么新意。

(4) Cloud Security Posture Management（云安全配置管理）

CSPM 是跨 IaaS 和 PaaS 来工作的，是对基础设施安全配置进行分析与管理，这个不是新概念。

(5) Simplify Cloud Access Controls（简化云访问控制）

企业希望能够在多个云服务中实现中心化策略和治理对于用户、设备、用户活动和敏感数据的可见性。

(6) DMARC（基于域的消息认证报告和一致性）

DMARC 是一种使电子邮件发送者和接收者更轻松的方法，确定给定消息是否合法地来自发送者。

(7) Passwordless Authentication（无密码认证）

完全消除密码目前看来还不太可能，但减少对密码的依赖已经是可行的，可以增加信任并改善用户体验。

(8) Data Classification and Protection（数据分级与保护）

不同用户分类分级的策略差异比较大，需要组织确定后通过技术来实现。这个国内情况貌似也差不多，分类分级打标签就是一大难题。

(9) Workforce Competencies Assessment（员工能力评估）

数字化商业要求我们有合适的人在正确的岗位上扮演正确的角色，拥有正确的技能和能力。看来安全人才缺口是全球性问题。

(10) Automating Security Risk Assessments（自动化安全风险评估）

只有 58%的安全负责人对重要的新项目进行风险评估，自动化风险评估会简化了 IT 交付。

https://www.freebuf.com/articles/network/249842.html