[公开]360BEST-DST-0-003-20200727

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 3 期 2020 年第 3 期

（2020.7.20-2020.7.26）

大数据协同安全技术国家工程实验室

全球动态

1、7 个 VPN 服务导致两千万名用户数据泄露

2020 年 7 月 21 日，来自 vpnMentor 的安全专家发现 7 个免费的 VPN 将 1.2TB 私人用户数据暴露在网上，其中包括多达 2000 万名 VPN 用户的个人身份信息。受影响的 VPN 服务包括 UFO VPN、FAST VPN、FREE VPN、SUPER VPN、Flash VPN、Secure VPN 和 Rabbit VPN。

https://securityaffairs.co/wordpress/106181/data-breach/7-vpn-data-leak.html

2、阿根廷电信 1.8 万台计算机感染勒索软件

2020 年 7 月 21 日，阿根廷电信公司遭到勒索软件攻击，短短一个周末，就造成约 1.8 万台计算机被感染，勒索方要求阿根廷电信提供 750 万美元的赎金。截至目前为止，阿根廷电信运营的许多网站都因为此次勒索攻击事件而导致脱机。

https://www.secrss.com/articles/24074

3、无锡警方发现 500 多万条公民个人信息遭泄露

2020 年 7 月 24 日，据央视财经报道，江苏无锡警方破

获一起非法侵犯公民个人信息案，涉案公民个人信息达 500 多万条。涉案人员来自家装业、房产中介业、地产开发业等多个行业，遭泄露公民个人信息量达 500 余万条。

https://www.fx168.com/fx168_t/2007/4038321.shtml

4、DNA 分析服务 GEDmatch 遭遇数据泄露，暴露了 130 万份资料

2020 年 7 月 24 日，据外媒 Techspot 报道，一起重大安全漏洞事件促使 DNA 分析服务 GEDmatch 的所有者将网站下线。经调查发现有一个 DNA 资料的宝库被提供给执法部门搜索（并延伸到该服务的所有其他用户），该事件暴露了其数据库中不少于 130 万条 DNA 记录。

https://www.cnbeta.com/articles/tech/1007147.htm

5、科技独角兽 Dave 承认 750 万名用户的记录被泄露

2020 年 7 月 26 日，数字银行应用程序和科技独角兽 Dave.com 在黑客公开论坛上发布了 7,516,625 位用户的详细资料后，确认存在安全漏洞。

https://securityaffairs.co/wordpress/106364/data-breach/dave-com-data-breach.html

业界观点

1、微软发布 Double Key Encryption 新特征

2020 年 7 月 21 日，微软官方发布了 Microsoft 365 新的安全特征 Double Key Encryption（双密钥加密）。双密钥加密使用了 2 个密钥来保护数据，其中一个密钥是用户控制的，另一个密钥安全地保存在 Microsoft Azure 中。

https://www.4hou.com/posts/vDw0

2、NIST 公布第三轮后量子密码竞赛入围算法

2020 年 7 月 22 日，NIST 正式公布了第三轮后量子密码竞赛的 7 个候选算法。

PKE/KEM：CRYSTALS-KYBER（基于格）、NTRU（基于格）、SABER（基于格）、Classic McEliece（基于编码）

数字签名：CRYSTALS-DILITHIUM（基于格）、FALCON（基于格）、Rainbow（基于多变量）

此外，以下 8 种算法将进入备选组。

PKE/KEM：BIKE、FrodoKEM、HQC、NTRU Prime、SIKE；数字签名：GeMSS、Picnic、SPHINCS+

https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement

3、Gartner 2020 年规划指南：安全和风险管理

Gartner 建议：组织必须在坚实的安全基线基础上，继续推进其安全规划和安全架构计划。安全和风险管理趋势可总结如下：（1）全球合规和风险环境的重大变化，持续影响企业安全规划；（2）安全监控和响应将继续依赖通过内部技能和托管服务提供的自动化和分析；（3）安全架构将受到集成化安全平台方法的推动；（4）容器、DevSecOps、混合云和多云将改变基础设施安全架构和管理；（5）生态环境将巩固以数据为中心的安全架构和应用程序安全的需求；（6）移动设备、物联网、代理和 SaaS 将推动原生安全能力和附加组件的扩展。

https://www.secrss.com/articles/17506

4、可信人工智能面临的数据安全问题

人工智能的安全问题分成两部分：第一类是数据安全，第二类是模型安全。针对于数据安全方面可以总结出三种问题。第一种，本身数据质量有问题。第二种，数据保护。第三种，数据隐私。

https://www.secrss.com/articles/24038

5、解决数据安全的新方法—机密计算

机密计算是一种突破性技术，可以完成对数据的加密，是针对数据在使用过程中的安全问题所提出的一种解决方案。它是一种基于硬件的技术，将数据、特定功能、应用程序，同操作系统、系统管理程序或虚拟机管理器以及其他特定进程隔离开来，让数据存储在受信任的执行环境（TEE）中，即使是使用调试器，也无法从外部查看数据或者执行操作。

https://fortune.com/2020/07/20/confidential-computing-cloud-hackers/

6、隐私计算能长出新的大数据平台

隐私计算，广义上是指面向隐私保护的计算系统与技术，涵盖数据的产生、存储、计算、应用、销毁等信息流程全过程，想要达成的效果是使数据在各个环节中“可用不可见”。目前最先落地于金融、医疗等行业。在数据合规的要求下，谁能汇聚海量优质的数据源，并以高效的技术/产品方式帮助需求方提取可用数据，实现数据价值，谁就可能成为新的大数据平台。

https://www.36kr.com/p/801141060510982

7、Polymer 推出的解决方案可以自动编辑协作工具中共享的敏感数据

2020 年 7 月 22 日，协作安全初创公司 Polymer 宣布正式启动一个解决方案，该解决方案可以自动检测并编辑用户在流行的协作工具中共享的敏感数据。Polymer 旨在实时检测和编辑敏感材料，包括个人身份信息（PII），健康信息，财务数据，ID 信息，网络详细信息以及加密货币地址和私钥。当用户通过一种受支持的协作工具共享此类信息时，Polymer 会自动编辑敏感信息，并确保只有经 Polymer 管理仪表板授权的用户才能访问未编辑的信息。

https://www.securityweek.com/polymer-launches-solution-avoid-data-leaks-collaboration-tools?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29

8、考虑到数据安全，如何选择最佳的云解决方案

随着越来越多的公司企业开始采纳公有云和私有云解决方案，其中的数据安全问题越来越被重视。在具体应用场景下如何选择一个最佳的云解决方案主要考虑以下几点：

- 考虑当前数据和未来服务扩展可能会纳入的数据。如果采用私有云和公有云并存的混合环境，还得考虑数

据在两个环境中“泄露”的风险。

- 服务提供商切实提供的安全服务及其历史安全响应效果。
- 自家公司或单位用于维护该服务的安全技术/工具集的能力和覆盖范围。

https://www.aqniu.com/news-views/56853.html