[公开]360NELab-DST-0-063-20211025

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 63 期 2021 年第 39 期

（2021.10.18-2021.10.24）

大数据协同安全技术国家工程实验室

目录

政策形势

1、习近平：把握数字经济发展趋势和规律 推动我国数字经济健康发展

新华社北京 10 月 19 日电 中共中央政治局 10 月 18 日下午就推动我国数字经济健康发展进行第三十四次集体学习。

中共中央总书记习近平在主持学习时强调，近年来，互联网、大数据、云计算、人工智能、区块链等技术加速创新，日益融入经济社会发展各领域全过程，数字经济发展速度之快、辐射范围之广、影响程度之深前所未有，正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。要站在统筹中华民族伟大复兴战略全局和世界百年未有之大变局的高度，统筹国内国际两个大局、发展安全两件大事，充分发挥海量数据和丰富应用场景优势，促进数字技术与实体经济深度融合，赋能传统产业转型升级，催生新产业新业态新模式，不断做强做优做大我国数字经济。

https://xhpfmapi.xinhuaxmt.com/vh512/share/10329252?channel=weixin

2、工信部：督促企业建立个人信息保护“双清单”制度

2021 年 10 月 19 日，工信部新闻发言人、信息通信管理

局局长赵志国在国新办发布会上表示，下一步将启动为期半年的信息通信服务用户感知提升专项行动，督促企业建立个人信息保护“双清单”制度（已收集个人信息清单和与第三方共享个人信息清单）。同时，优化隐私政策和权限调用提示，充分保障用户知情权和选择权，进一步提升用户获得感和安全感。

https://mp.weixin.qq.com/s/UyOKy1gMFOGT8XV9fRDnKw

3、11 省份已出台“数据条例”

加强数据安全保护和监督管理制度建设，各地已经行动起来。目前，已有山东等 11 个省份出台了与数据相关的条例（包括大数据条例、数据条例、数字经济条例，统称为“数据条例”），上海市正在制定数据条例。数字化发展时代，全社会数据总量将爆发式增长，而打通数据流动通道，提供快速的数据分析能力，离不开构建完善的数据产业生态，建设数字基础设施势在必行。

https://mp.weixin.qq.com/s/bYV91KvPRjdDjSIckleraQ

4、国信安标委征求《信息安全技术 汽车采集数据的安全要求》国家标准（征求意见稿）意见

2021 年 10 月 19 日全国信息安全标准化技术委员会归口

的《信息安全技术 汽车采集数据的安全要求》国家标准已形成标准征求意见稿，并面向社会公开征求意见。

https://mp.weixin.qq.com/s/ApwYtHeiIiRFd_Gw4OCbbA

5、温州发放首份个人数据资产云凭证

10 月 21 日，温州举行数字化改革惠企利民典型应用集中启用仪式。现场，温州依托“个人数据管家”，实现数据授权使用，发放首份个人数据资产云凭证。温州市大数据发展管理局局长顾威介绍，这是温州大力探索数据要素市场化配置的有益尝试。通过“个人数据管家（个人数据宝）”，温州已经将 57 个领域的个人数据开放给用户本人，实现数据的便捷查询和授权使用。

http://dsjj.wenzhou.gov.cn/art/2021/10/21/art_1229002337_58998588.html

业界观点

1、360 杜跃进：构建面向数智时代的网络安全能力体系

数智时代的世界有三大核心特点，分别是**软件定义、泛在互联、数据驱动**。这就意味着，数智时代的网络攻击是无死角、跨时空，而且极其隐蔽。随之而来的新威胁和大挑战体现在**战场大、对手大、目标大、布局大、手法大、危害大、挑战大**七个层面。目前，随着数据化的深化、智能化的开始，网络安全也表现为从 ICT 的安全，到数字世界的安全世界。

未来安全，就是**基于数据、依靠协同、构建通过运营持续进化的安全能力体系**。其核心是满足新时代要求的处理中枢——安全大脑。安全大脑以安全大数据为基础的，具备安全大数据的分析能力，可以通过人机结合的方式不断积累和更新安全知识和经验。安全大脑并不具备预设的特定功能，而是通过与其他所有安全相关组件连接通信，借助强大的中枢分析能力将各安全组件有机地组织起来，实现智能协同。

https://mp.weixin.qq.com/s/nUfxQCOMt0jvGnxetaIV3g

2、Gartner 发布 2022 年 12 个重要战略技术趋势

据 Gartner 官网 10 月 19 日消息，Gartner 发布了企业机构在 2022 年需要探索的 12 种重要战略技术趋势，聚焦工程

化信任、塑造变化和加速增长三大主题。

12 种重要趋势包括可用于创建代码、药物研发、伪造身份的生成式人工智能；整合并动态改进机构数据的数据编织；分布式企业；云原生平台（CNP）；自治系统；决策智能；组装式应用程序；超级自动化；隐私增强计算；网络安全网格；可实现人工智能模型操作化的人工智能工程化；结合客户体验、员工体验、用户体验和多重体验的全面体验等。

https://mp.weixin.qq.com/s/i6qX0RUH2vrlw81N5s1xXw

3、2021 年上半年全球 DDoS 攻击同比增长 11％

近日，国际知名公司 NETSCOUT 公布其调查报告结果显示，2021 年上半年，网络罪犯发动了约 540 万次分布式拒绝服务（DDoS）攻击，比 2020 年上半年的数字增长 11%。数据预测指出，2021 年是全球 DDoS 攻击超过 1100 万次的又一创纪录的一年。

2021 年上半年，在 Colonial Pipeline（美国最大燃油管道公司）、JBS（全球最大肉食加工供应商）、Harris Federation（英国非营利多学院信托机构）、澳大利亚广播公司第九频道、CNA 金融和其他几起高调攻击之后，DDoS 和其他网络安全攻击的影响已在全球范围内显现出来。许多当地政府正在积极推出新的计划和政策，以抵御攻击，而各地安全部门

正在发起前所未有的合作努力来应对危机。

https://xw.qq.com/cmsid/20211021A0368H00?pgv_ref=baidutw%0D%0A

4、用零信任强化鉴别和访问控制机制，助力数据安全

《中华人民共和国数据安全法》中明确指出数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。而企业上云、数字化转型过程中由于传统安全边界的逐渐消失，暴露出众多的安全威胁问题。零信任的无边界安全模型，“持续验证、永不信任”的安全模型为我们提供了新的安全思路，也是对现阶段安全防护手段的重要弥补措施。

零信任作为新一代的网络安全防护理念，默认不信任企业网络内外的任何人、设备和系统，基于身份认证和授权重新构建访问控制的信任基础，从而确保身份可信、设备可信、应用可信和链路可信。基于零信任原则，可以保障办公系统的三个“安全”：终端安全、链路安全和访问控制安全。

零信任安全只是理念，企业实施零信任安全理念需要依靠技术方案才能将零信任真正落地。在 NIST《零信任架构标准》白皮书中列举了 3 个技术方案，可以归纳为“SIM”组合：SDP，软件定义边界、IAM，身份权限管理和 MSG，微隔离。

https://www.secrss.com/articles/35289

5、2022 年全球数字趋势洞察：复杂的 IT 基础设施形成安全风险

咨询公司普华永道的最新数据显示，过半数高管担心应报告的攻击会持续增长，超过三分之二的公司计划增加 2022 年网络预算，从而更好地保护其系统和数据。

报告称，四分之三（75%）的高管承认其所在企业的基础设施变得过于复杂，而几乎相同数量的受访者认同复杂性导致了风险水平增加至令人担忧的程度。总体而言，高管们担心复杂性主要可导致数据泄露和财务损失，而且还会阻碍创新和破坏运营弹性。

根据《2022 年全球数字信任洞察》报告，超过一半的公司在云安全、安全意识培训或端点安全方面投入了资金和人力物力，但只有大约三分之一的公司切实从这方面投资上获得了收益。

https://www.secrss.com/articles/35244

安全事件

1、黑客出售 5000 万莫斯科司机的数据

2021 年 10 月 24 日，黑客正在一个黑客论坛上以 800 美元的价格出售一个包含 5000 万条莫斯科司机记录的数据库。黑客声称已从当地警方的内部人员那里获得数据，他们发布了一个数据库记录样本，其中包含汽车型号、注册和 VIN 号、注册日期、发动机功率、车主姓名、日期出生，电话号码。被盗数据跨越 2006 年和 2019 年，当地媒体已证实其真实性。黑客还向购买数据库的人提供包含 2020 年信息的文件。

https://securityaffairs.co/wordpress/123711/data-breach/moscow-drivers-data-leak.html

2、宏碁服务器再次被窃，超 60GB 用户数据或被出售

2021 年 10 月 14 日报道，宏碁服务器数据再次被窃，该公司数百万客户的数据目前被扣押。超过 60GB 的委托人、客户和零售商的信息现在掌握在黑客手中，他们正在寻找买家出售这些数据。此次泄密主要影响印度的客户，这是宏碁在过去七个月里遭遇的第二次黑客攻击，前一次是在 3 月份，据 REvil 黑客组织声称，那次攻击涉及创纪录的 5,000

万美元赎金。

https://securityaffairs.co/wordpress/123616/data-breach/acer-suffers-second-data-breach.html

3、数据分析公司披露了 200 万 Instagram 和 TikTok 用户的数据

2021 年 10 月 21 日，由阿努拉格·森(anuragsen)领导的网络安全团队发现了社交媒体分析网站 igblade.com 的一个不安全搜索服务器。该服务器存储了数百万社交媒体用户的数据。这些数据来自 tiktok 和 instagram。据报道，至少有 260 万用户的资料被泄露，相当于超过 3.6GB 的数据。

https://www.hackread.com/data-analytics-firm-expose-instagram-tiktok-users-data/

4、阿根廷政府公民数据库疑全部泄露

2021 年 10 月 18 日，据外网报道，一名黑客入侵了阿根廷政府的 IT 网络，并窃取了该国所有人口的身份证详细信息。这名黑客在推特上泄露了阿根廷总统、球星梅西和阿圭罗等数十个当地名人的身份证信息，并在黑客论坛上兜售阿根廷公民身份信息查询权限。

根据黑客在线提供的样本，他们现在可以访问的信息包

括全名、家庭住址、出生日期、性别信息、身份证签发和到期日期、劳工识别代码和政府照片身份证等。

https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population/

5、SCUF 游戏商店确认其 3.2 万客户的信息已经泄露

2021 年 10 月 22 日，SCUF 游戏商店确认被黑客入侵并被窃取 32,000 名客户的信用卡信息。SCUF 游戏商店为 PC 和控制台制作高性能和定制的游戏控制器，由专业和休闲游戏玩家使用。攻击者将基于 javascript 的脚本，注入被称为信用卡略读器(又名 magecart 脚本)的网络商店，使他们能够获取并窃取客户的支付和个人信息。攻击者随后在黑客或卡片论坛上把它卖给其他人，或在各种金融或身份盗窃欺诈计划中使用它。因此，恶意脚本就被部署到 scuf 游戏的在线商店中。

https://www.bleepingcomputer.com/news/security/scuf-gaming-store-hacked-to-steal-credit-card-info-of-32-000-customers/