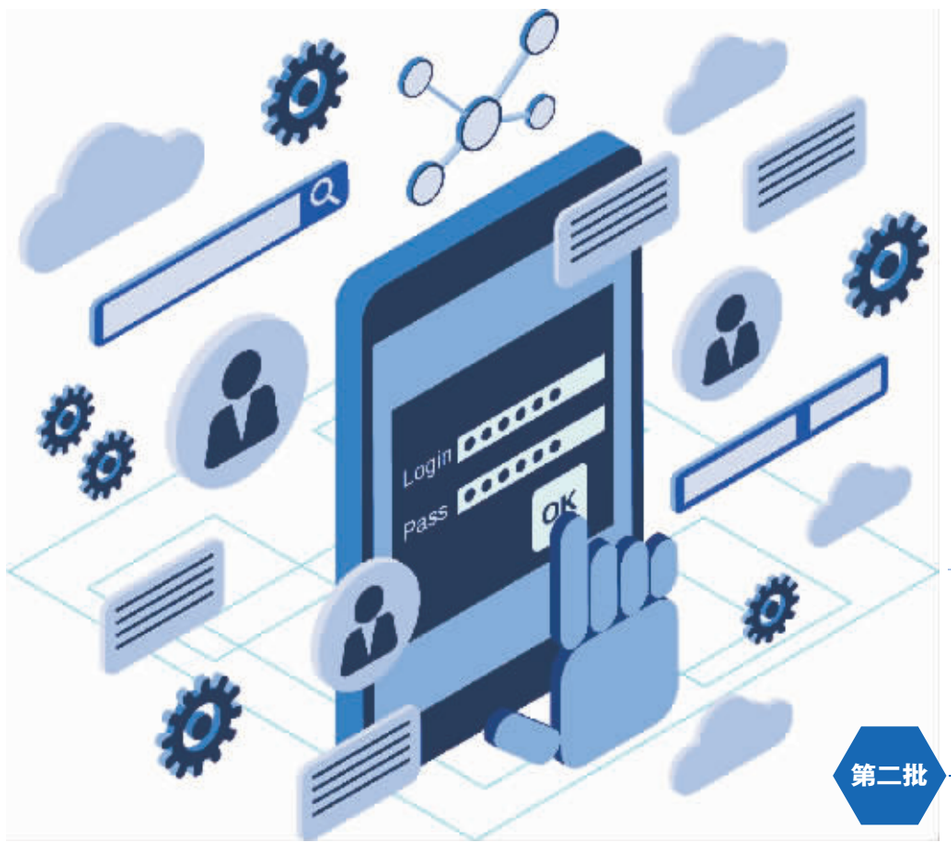
编辑 赵天舒 美编 李烝 责校 杨志强 电话:64101946 bbtzbs@163.com

3万条信息泄露 微软AI出岔子



自从生成式人工智能热潮兴起以来，有关数据安全性的争议就始终不断。事实证明，即便是“头部大厂”微软也有数据泄露的风险。据一家网络安全公司的最新研究显示，微软公司的人工智能研究团队数月前就曾意外在软件开发平台GitHub上泄露了大量私人数据，其中涵盖了3万多条微软团队的内部信息。虽然没有涉及用户信息，但正如在上周一场以管理人工智能为主题的闭门论坛上特斯拉CEO马斯克所说，“对我们来说，重要的是要有一个裁判”。

>>> 已承诺管控AI风险的公司

第一批：亚马逊 | 谷歌 | OpenAI | 微软 | Anthropic | Inflection | Meta

第二批：Adobe | Cohere | IBM | 英伟达 | Palantir | Salesforce | Scale AI | Stability

访问权限设置错误

一个小小的设置失误，导致微软在近三年的时间里将大量内部数据暴露在外。当地时间9月18日，据网络安全公司Wiz报告，公司在对云托管数据的泄露问题进行持续调查时，发现微软AI研究团队在发布开源数据时意外泄露38TB的隐私数据，其中包含3万多条员工内部信息。

据了解，导致该次数据泄露的源头是微软在GitHub存储库中提供了一个属于微软云存储系统Azure Storage的网址链接，可以用来下载开源代码和用于图像识别的AI模型。然而，由于微软的AI开发人员在网址中包含了一个过于宽松的共享访问签名（SAS）令牌，此链接竟被设置成授予整个存储账户的权限。也就是说，点进该链接的任何人都能访问与之相关的存储账户的全部内容。

更可怕的是，该链接给予访问者的权限不是只能观看、不能修改的“只读”，而是“完全控制”，意味着任何人都有可能在整个账户中删除、替换或添加恶意内容。

在受到影响的全部数据中，包括了两名微软员工的个人电脑备份，还有用于微软服务的密码、秘钥以及Teams上来自359名微软员工的超3万条内部群聊消息。

Wiz表示，这个网址链接从2020年就开始暴露数据，直到Wiz发现该问题并在今年6月22日和微软分享了研究成果。微软在两天后的6月24日撤销了有问题的SAS令牌，并在今年8月16日完成了对组织内部潜在影响的调查。

对于此事，微软发言人表示，微软已确认没有用户数据遭到泄露，也没有其他内部服务受到威胁。微软安全响应中心在当日发布的博客文章中表示，收到Wiz的研究结果之后，他们已经改进了GitHub的秘密扫描服务，该服务能够监控所有公开的开源代码改动，其中包括那些过于宽松的SAS令牌。

AI安全如何确保

事件再一次引起了对于AI数据安全问题的关注。Wiz的联合创始人兼首席技术官阿米·卢特瓦克（Ami Luttwak）指出：“很多开发团队都需要处理大规模的数据，需要与同事共享数据或在公共开源项目上进行合作，像微软这样的案例将会变得越来越难以监控和避免。”

一位从事IT研发的工程师也对北京商报记者表示，大模型时代需要跑通的数据更多，人工智能企业需要收集和利用大量数据来训练算法模型，由此出现漏洞的概率也就更大。

在2021年，Wiz就曾指出过微软Azure基础设施中的一个“超级漏洞”，其开源应用Jupyter Notebook功能中的一系列错误配置让黑客能够访问、修改和删除数千名Azure客户的数据。随后，微软发布声明称该问题已得到解决，并用电子邮件通知了数千名受其影响的云客户。

在天使投资人、资深人工智能专家郭涛看来，人工智能行业保护用户隐私和数据安全需要多方面协同发力，一方面，人工智能技术公司需要遵循严格的隐私数据保护相关的法律法规，采取相应的措施和技术手段来确保数据的安全性、完整性和机密性，如匿名化、去标识化等技术来保护用户因素和数据安全；另一方面，提高数据利用的透明度，向用户解释如何收集和使用数据，以及为什么需要这些数据，用户有权决定是否愿意提供这些数据。

“要有一个裁判”

与此同时，监管部门也正在努力解决如何减轻风险。上周，美国商务部长雷蒙多等政府高官在白宫召集AI行业高管，宣布Adobe、Cohere、IBM、英伟达、Palantir、Salesforce、Scale AI和Stability 8家公司承诺，采取自愿监管措施管理AI技术开发风险，包括在推出前展开安全测试、构建将安全放在首位的系统、为AI生成内容添加数字水印等。

具体来看，上述8家公司承诺：在发布AI系统前进行内部和外部安全测试、对网络安全和内部威胁保障措施投资、推进第三方发现和报告AI系统存在的漏洞等。

此外，8家公司还承诺，对AI生成的内容加上水印以防止虚假信息的传播，公开报告安全风险和社会风险，开发有助于解决癌症预防、气候变化等社会挑战的AI系统等。

这8家为第二批承诺管控AI风险的公司。今年7月，已有7家领先的人工智能公司——亚马逊、Anthropic、谷歌、Inflection、Meta、微软和OpenAI自愿承诺，将帮助推动AI技术安全且透明地发展。

当天，马斯克、微软公司联合创始人比尔·盖茨和Meta首席执行官扎克伯格等科技公司大佬还受邀参加了一场人工智能峰会，商讨未来人工智能的监管方式。

作为推动人工智能立法的一部分，美国参议院多数党领袖查克·舒默组织了这次私人论坛。他表示，他问了在场的每个人——包括约20名科技高管、倡导者和怀疑论者——政府是否应该在人工智能的监督中发挥作用，“每个人都举手了，尽管他们有不同的观点，”他说。

在国会方面，虽然国会议员也同意需要加强立法，但对于具体行动也一直没有达成共识。一些国会成员担心监管会“过度”，而另一些议员则认为没有足够的监管将难以发现“潜在风险”。

“人工智能出错的后果是严重的，所以我们必须积极主动，而不是被动反应。”马斯克在离开前表示，需要一个监管机构确保企业采取安全、符合公众普遍利益的行动。“对我们来说，重要的是要有一个裁判。”

北京商报记者 方彬楠 赵天舒

聚焦 Focus

降价拉低盈利预期 特斯拉市值受拖累

美国时间9月18日，截至美股收盘，特斯拉股价下跌3.32%，每股报价265.28美元。一夜之间，特斯拉市值蒸发近290亿美元（约合2117亿元人民币），当前市值8419.97亿美元。在外界看来，特斯拉市值下跌背后与高盛下调其盈利预期有关。因担忧如果特斯拉继续降价将影响汽车毛利，高盛下调特斯拉目标价至275美元。

高盛分析师马克·德莱尼在一份报告中提出：“我们认为，特斯拉可能会在2024年继续下调价格以支持更高的销量，这将抵消其通过成本削减带来的收益。”

同时，来自金融数据供应商FactSet的数据显示，分析师一致认为特斯拉2023年利润将下降17%至每股3.36美元。德莱尼表示，售价下降对汽车毛利产生影响，由此下调特斯拉2023年和2024年每股收益的预期，将2023年特斯拉每股收益预期从3美元下调至2.9美元，并将2024年的每股收益预期从4.25美元下调至4.15美元。

值得一提的是，由福特、通用和Stellantis与美国汽车工人联合会（UAW）在薪资待遇分歧上导致的美国三大车企工人罢工已进入第四天。有报道称，此次罢工如果持续时间较长，将产生重大影响，相关零部件企业也将面临没有需求而受到连带停产风险。不过，韦德布什证券公司分析师丹·艾夫斯在一份研究报告中表示：“如果发生罢工，美国汽车产量将受影响，但竞争对手的停产将对特斯拉有利。”据了解，相比福特、通用和Stellantis等UAW车企，特斯拉等非UAW车企所支付的劳动成本更低。而特斯拉CEO埃隆·马斯克则一直反对工会组织，并直言“工会组织会拖垮企业效率”，导致特斯拉与UAW的关系剑拔弩张。此外，本次美国三大车企工人罢工后，马斯克更以“特斯拉支付给工人的工资更多”的表态暗讽UAW。

不过，美国三大车企为特斯拉带来的利好消息并未在资本市场显现，反而在多次降价下，市场对其盈利能力表示担忧。今年以来，特斯拉多次通过调节价格方式冲量。据统计，在美国市场，作为特斯拉主力车型的Model 3入门版车型售价今年1月起下降14%；二季度Model 3车型平均价格约4.56万美元，同比下降20%。同时，数据显示，今年二季度，特斯拉交付量为46.61万辆，同比增长约83%。对此，市场层面曾预测，特斯拉将交付44.5万辆汽车。此前，据统计，近一年特斯拉的交付增长率始终低于五成。频繁的价格调整让特斯拉二季度销量增长超八成并拉动营收增长。

但销量营收增长下，今年一季度，特斯拉净利润同比下滑超24%。今年二季度，特斯拉营业利润为23.99亿美元，同比下降3%，环比下降9.9%。同时，今年二季度总体毛利率为18.2%，低于分析师预期的18.8%，为四年以来最低水平。特斯拉在一份股东报告中解释称：“所销售汽车的平均价格降低以及提高内部设计的4680电池产量的成本高昂等因素，导致二季度利润率下降。”在中国汽车流通协会专家委员会成员颜景辉看来，今年初特斯拉便打出降价牌，在提前为年销增长50%目标收割销量的同时，价格下探势必将影响其盈利能力。

高盛对于特斯拉可能再次调整价格的担忧并非空穴来风。在财报电话会议上，马斯克曾直言：“牺牲车辆利润率换取更多产量‘说得通’，若整体经济环境不稳定，特斯拉还将继续降价。”同时，马斯克表示，要用长期眼光投资特斯拉，要像巴菲特那样进行价值投资，并预计特斯拉价值有增长5倍甚至10倍的潜力。

今年9月，特斯拉正式开启新款Model 3预售，相比老款车型，新款售价上调。高盛方面表示，新款Model 3涨价仅能部分抵消此前降价的影响，从而导致特斯拉产品组合的平均售价下降，影响毛利率。值得一提的是，今年9月1日新款Model 3预售发布时，特斯拉同时下调Model S和Model X在中国市场的售价。

此外，对于三季度价格调整，德莱尼认为：“即使降价，三季度特斯拉的销量仍将低于预期。”不过，随着特斯拉推出新款Model 3 Highland并考虑Model S和Model X两款车降价后的销量增长，德莱尼预计，四季度特斯拉销量将出现反弹。“今年特斯拉的交付量预期将达184.2万辆。”他表示。

北京商报记者 刘洋 刘晓梦

·图片新闻·

33万亿美元 美国国债规模破纪录

人们经过美国纽约曼哈顿的“国债钟”。新华社/图

美国财政部网站日前更新的信息显示，美国联邦政府债务规模突破33万亿美元，达到33.04万亿美元。美国国债呈加速上升势头。

此前，根据美国财政部网站今年6月16日更新的信息，联邦政府债务规模突破32万亿美元，达到32.039万亿美元。美国联邦政府债务规模突破32万亿美元的时间比新冠疫情前的预测提前了9年。

美国联邦政府债务今年1月已触及31.4万亿美元的债务上限，财政部随即采取“非常规措施”以避免债务违约。为此，两党展开数月激烈博弈，于5月底就联邦政府债务上限和预算达成初步一致，并最终形成相关法案，获国会通过。

美国总统拜登6月3日签署关于联邦政府债务上限和预算的法案。这一法案暂缓债务上限生效至2025年年初，并对2024财年和2025财年的开支进行限制，是自二战结束以来美国第103次调整债务上限。

美国联邦政府债务规模于2022年2月初突破30万亿美元，预计到2030年将超过50万亿美元。

据外媒报道，国债总额再创新高数据正值联邦支出再度引发争议、政府面临停摆之际，美国财政前景堪忧。据悉，如果国会无法在9月30日前通过长期的拨款法案或短期支出法案，政府将再度面临停摆危机。 **据新华社**