新闻热线：010—58884062
E-mail：adaxuqian@126.com
■责编 许 茜
科技日报 2018年8月1日 星期三

工业数据：黑客盯上的又一块“肥肉”

数据平台存在的漏洞是导致此次事件发生的根本原因。近年来，工业数据平台被曝出的漏洞日益增多，且大量集中在装备制造、交通、能源等重要领域。一些黑客正是利用这些漏洞，窃取了大量的工业信息。

实习记者 于紫月

包括克莱斯勒、福特、特斯拉等全球100家车企的超过47000个机密文件遭外泄，这一被媒体称为迄今为止最严重的工业数据“车祸”于近日发生。

据报道，数据泄露的源头指向了这些车厂共同的服务器提供商Level One Robotics and Controls（以下简称Level One），泄露的数据包括产品设计原理图、装配线原理图、工厂平面图、采购合同等敏感信息。

“这只是全球近年来频发的工业信息安全事故的缩影。”7月30日北京理工大学网络攻防对抗技术研究所所长闫怀志在接受科技日报记者采访时说，从全球发展趋势来看，工业互联网和工业数据日益成为黑客攻击的重点目标。

那么，到底谁是这次工业数据泄露事件的罪魁祸首呢？我们又该如何有效防止类似事件的发生呢？

访问不设限酿“车祸” 平台漏洞是祸首

“车祸”主角Level One是一家数据管理平台公司，它主要提供基于客户原始数据的定制化服务。

“Level One在使用远程数据同步工具rsync处理数据时，备份服务器没有限制使用者的IP地址，并且未设置身份验证等用户访问权限，因此任何人都能直接通过rsync访问备份服务器，这是导致事故发生的主要原因。”7月30日宝沃汽车（上海）有限公司总工程师刘凯在接受科技日报记者采访时说，“由于业务扩展需要，如今越来越多的第三方公司获得了车企的访问权限，车企数据泄露的风险也就随之增加。”

在闫怀志看来，数据平台存在的漏洞是导致此次事件发生的根本原因。“近年来，工业数据平台被曝出的漏洞日益增多，尤其是工业控制系统内的安全漏洞层出不穷，且大量集中在装备制造、交通、能源等重要领域，严重威胁国家信息基础设施安全。一些黑客正是利用这些漏洞，窃取了大量的工业敏感信息。”闫怀志说。

自2015年以来，全球每年发生的工业信息安全事件接近300起，工业领域已成为网络攻击“重灾区”。

国家工业信息安全发展研究中心监测数据结果显示，我国3000余个暴露在互联网上的工业控制系统，95%以上都存在漏洞，可轻易被远程控制，约20%的重要工控系统可被远程入侵并完全接管。

“目前很多工业系统和设备没有防护软件，也未安装杀毒系统，一旦上了网就基本处于‘裸奔’状态。”一位业内人士表示，目前我国一些通信、能源、水利、电力等关键基础设施存在着较大的安全风险，而入侵和控制工业信息系统也已成为商业上打压竞争对手的不法手段。

企业安全意识薄弱 相关人才储备匮乏

“目前，我国很多地区、部门、工业企业对工业数据安全重视不够，重发展轻安全，不重视漏洞、修复不及时等现象普遍存在。”闫怀志说。

据360补天漏洞响应平台统计，在其涵盖的工业相关信息系统漏洞中，25.6%的漏洞未进行修复，一些漏洞的平均修复时间长达数月之久。

我国对工业信息领域安全的认识还处在初级阶段。2017年5月“Wanna Cry”勒索病毒事件暴发，微软在当年3月就发布了相应的安全漏洞补丁，但我国很多单位一直由于未及时打补丁，导致近30万台主机和电脑被感染。

直到今年，360公司还能监测到每天有近千台电脑感染此勒索病毒。

在企业中，因私人行为导致设备感染病毒的情况也较为多见。例如，个人通过工控设备违规上网，或是厂商的维护人员电脑感染病毒后造成设备系统全网感染等。

此外，我国工业企业目前的防护技术还较为落后。国家工业信息安全发展研究中心通过安全监测发现，工业企业信息安全应急备灾手段不足，约70%的被调查企业缺少完善的应灾备灾体系。

防护技术之外，我国在工业信息领域的核心产品自主可控度也较低。

国家工业信息安全产业发展联盟发布的《2017年工业信息安全态势白皮书》显示，国产数据库仅占据7%的低端市场，大量工控系统由外国厂商提供运行维护。我国部分企业不具备自主维护能力，而且缺乏对外国产品和服务的监管。

同时，人才匮乏也是导致工业信息安全技术薄弱的原因之一。“公共信息安全人才需掌握自动化和网络安全两个学科的知识和技能，这类人才缺口巨大。但目前在高校中尚没有设立工业信息安全领域硕士、博士的培养方向，工业信息安全从业人员几乎都是在实践中学习。”闫怀志说。

筑防线需多方合力 可借鉴欧盟做法

“工业大数据的共享是工业互联网应用的基础和灵魂，而工业数据安全及隐私保护又是一切应用的前提。”闫怀志建议，要想给工业信息构筑起一道“防线”，首先企业应树立信息安全与隐私保护意识。

闫怀志介绍，传统IT网络中的隐私规范，主要应用“告知与许可”原则，由信息所有者自行决定可否、如何且由谁来处理或利用其信息，信息隐私保护的责任方为信息所有者。在工业大数据和工业互联网领域，工业数据需要被多次使用，传统的“告知与许可”隐私保护机制不具备现实可行性，工业数据信息隐私保护的责任将由数据使用方来承担。这种方式下可采用的保护手段包括数据分类分级和数据脱敏等。

此外，掌握大量工业信息的数据平台也应肩负起管理的责任。“此前我国网络安全与信息平台监管主体不清晰，多头监管问题突出，信息系统平台安全监管不力甚至监管缺失的情况时有发生，特别是在工业互联网和工业数据安全保护方面表现得更为突出。”闫怀志表示，“平台应不断完善数据隐私保护以及网络安全策略，成立数据安全与隐私保护的专门负责机构或组织。”

360集团董事长兼CEO周鸿祎也强调了漏洞管理的问题。他认为，应建立漏洞管理全流程监督处罚制度，制定覆盖网络安全漏洞的发现、审核、披露、通报、修复、追责等全流程管理细则，强制要求漏洞必须及时修复，对漏洞修复时间以及违规处罚措施予以明确规定。此外，应建立监督检查机制和力量，及时发现未及时修复漏洞，追究相关单位和责任人责任。

中国政法大学法学院大数据和人工智能法律研究中心主任汪庆华教授则从立法角度给出了建议。他对科技日报记者说，我国在网络安全和信息保护方面的立法呈现出分散式立法、多头式监管的特点。目前，我国已经初步建立起了以《网络安全法》为中心的分散式信息保护和数据安全方面的法律体系，未来还需进一步加强相关立法工作。

在政府监管方面上，闫怀志认为，我国可参考借鉴欧盟出台《通用数据保护条例》（GDPR）的做法，提高对信息非法获取的惩戒力度。

“GDPR是与当前网络空间现状最为契合的数据保护条例，要求手握数据的企业和机构设立专门的数据保护官员来负责数据管理。我国也可适当借鉴，要求企业和机构设立类似职位。此外，GDPR不仅倒逼中国企业更加重视数据安全和隐私保护，而且也为中国数据安全工作提供了一种思路——中国也可以制定类似条例来维护我国企业和公民个人的数据安全，防止国内外机构非法滥用。特别是在工业互联网和工业数据安全保护方面，有针对性的制度已成为燃眉之急。”闫怀志说。

行业观察

二手交易平台藏陷阱 买家、卖家都可能被坑

随着移动互联网的发展，二手物品交易的跳蚤市场从线下转移到了线上。然而，看似双赢的交易方式背后却隐藏了不少“坑”：卖家故意引导买家脱离平台交易实施诈骗，买家收货之后找借口向卖家恶意砍价……究竟是买卖双方诚意不够、还是平台本身存有漏洞？二手交易平台又有哪些陷阱需要警惕？

现状：网上二手交易问题多多

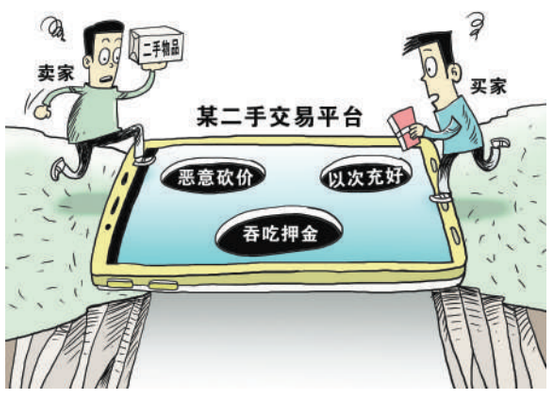
不少人在二手交易中有着不愉快的经历，快速增长的网上二手交易也问题多多。

汕头大学学生小余在赶集网上看到，原价2000多元的捷安特自行车只卖400多元，卖家还是“发烧友”，小余兴奋不已。

“发烧友卖的货肯定没错。”小余说，他确认了照片中车架上的品牌名后就果断地买了下来。可高兴没几天，自行车脚蹬就坏了。修车店的老板告诉小余：“这个车只有车架是这个品牌的，其他配件都被换成了不值钱的。”

“这个‘发烧友’卖家可能是假的。”网购达人小袁告诉记者，“自我包装”是二手交易平台卖家的惯用方式。在商品描述栏中写自我介绍时，卖家通常会把自己包装成“发烧友”“旅游爱好者”“大学生”等良好形象，这样在卖二手货时就更容易取信于人。

不仅买家可能被坑，卖家也有被骗的风险。西安某高校学生小九将一条码数偏大的裙子挂在二手交易平台“闲鱼”上售卖，一名买家看到后提出了“用同款小一码的裙子换”的建议，约定同时发货。几天后，对方收到了裙子并签收，但小九却发现对方一直“按兵不动”，迟迟不发货。最后小九找到买家电话，将相关法律法规告诉对方，对方这才同意将裙子寄回。



视觉中国

套路：以次充好、吞吃押金、恶意砍价

经调查发现，二手交易平台交易套路颇多：

第一，以次充好，偷换配件。厦门工学院学生小刘曾在闲鱼上购买了一个充电宝，商品描述和充电宝机身上写的都是2万毫安。但使用后小刘发现，这个充电宝给手机仅充一次电就会“精疲力尽”，还不如舍友5000毫安的充电宝电量足。小刘总结认为，二手交易平台上的手机、单车、充电宝等产品具有“外观迷惑性”，很多都是“看上去很美，一用就上当”。闲鱼客服对记者说，只要商家卖的不是违禁品，就可以在平台上发布。

第二，转场交易，吞吃押金。记者调查到，一些受访者被骗后面临申诉难，不少是由于交易脱离了原本的平台。安徽阜阳某中学的小张在转转上看到一部价值900元的小米手机，卖家说自己急需用钱，价格可降至800元，前提是小张要先用微信转账400元当作“预付款”，余款等货到结清。小张转账后，却迟迟没有收到手机。

第三，货物到手再砍价。广东的石先生就有被买家恶意砍价的经历，他曾在转转上以150元的价格售卖一部手机，一名买家很快就下单，并付钱到交易平台。但买家收到货后，却以手机内部防水标签变红为由，要求石先生退还80元。石先生很不满意，因为他的手机根本就没有进过水，便向客服申请仲裁，客服回复称要两人自行协商解决。苦于没有留存证据，石先生和买家僵持一周后，无奈同意了买家的请求。

“我查了他的买卖记录，发现买家是个手机贩子，挑毛病把我150元的手机砍到70元钱，又转手200多元卖了出去。”石先生说。

建议：完善买卖双方信誉评价体系

中国人民大学世界经济研究中心研究员赖明明认为，二手市场具有“柠檬市场”特点，即信息不对称，产品的卖方对产品的质量拥有比买方更多的信息，这导致交易中容易出现欺诈行为。

“二手交易平台对商品的真假负有相应审查义务及法律责任。”赖明明认为，真正合理可行的做法是，交易平台与二手商品售卖方共同担责，当出现贩卖假货等情况时，交易售卖方担主要责任、平台担次要责任，具体分责比率可进一步商榷。

北京市法学会电子商务法治研究会会长邱宝昌说，无论买家和卖家，当权益受到损害时，都可以先和交易对象协商，协商不成可以向平台投诉，之后可以向市场监管部门、消费者组织投诉，或者提起法律诉讼。邱宝昌表示，正在立法进程中的电子商务法有望进一步规范线上二手交易市场，强化平台经营者的责任，更好地保障交易双方的权益。（据新华社）

我国平均网速2.38Mbps？专家：不足为信

第二看台

本报记者 付丽丽

网速测试的结果不仅与测速方法、地点和数据来源等客观因素有关，同时还易受到一些“主观”因素的影响。

前不久，有媒体报道，著名统计机构M-Lab联合多家机构对2017年5月30日至2018年5月29日期间的全球1.63亿个独立网速测试进行了分析。结果显示，全球平均网速达到9.1Mbps（兆比特每秒）。在亚洲地区，韩国这次排在第30位，平均网速为20.63Mbps。中国的平均网速为2.38Mbps，排在第141位。

消息一出，引得中国网民莫名惊诧，事实真是如此吗？

测试结果与真实水平相差较多

“中国的平均网速为2.38Mbps，这个数字同中国用户的实际测速值及主观感受均有相当大的差距。”7月30日北京理工大学网络攻防对抗技术研究所所长闫怀志在接受科技日报记者采访时说。

闫怀志介绍，这个数字的主要提供方之一M-Lab是由美国新开放技术研究所、谷歌公司等机构共同建立的，是世界上最大的开源互联网测量组织之一。事实上，宽带网速测试的结果与测速方法、地点和数据来源等客观因素有很大关系，同时还易受到一些“主观”因素的影响。

“国外不同机构或组织测出的结果有时会相差巨大。比如，国际知名测速网站Ookla、Akamai同期公布的中国大陆平均网速分别为61.24Mbps、7.3Mbps，排名则分别为第23位、第74位。因此，单纯说中国的平均网速为2.38Mbps并不准确，根本无法客观公正地说明中国网速的情况，不足为信。”闫怀志说。

就此问题，一位不愿具名的业内人士向科技日报记者表示，目前并不知道M-lab是通过什么测量方法得到这个结果的。一般来说，网速指标测量会涉及非常多的因素，比如测试站点的分布、网络终端的接入模式等。

此前中国互联网络信息中心（CNNIC）曾发布第41次《中国互联网络发展状况统计报告》，报告中列出的2017年第三季度全国固定宽带网络下载的忙闲时加权平均下载速率为16.4Mbps，移动宽带通过4G访问互联网的平均加权速度为15.4Mbps。

“这两个结果与2.38Mbps也相差很多。总体而言，我国网络基础设施技术水平近几年已有较大的提升，尤其是部分发达省份的基础设施建设已达到了一个较高的水平。虽然少数经济落后地区因种种原因网络基础设施水平还有待提升，但M-lab给出的这个结果与我国目前网速的真实水平还是相差较大。”上述不愿具名人士说。

地区发展不均衡，我国网速仍有较大提升空间

“当然，M-Lab的网速报告也并非一无是处，至少它指出了一个事实，发达地区和欠发达地区网速差距正在扩大。”闫怀志说，我国网民规模接近8亿、世界第一，同时我国正处在宽带提速、5G商用在即的利好之下。但我国由于网络规模巨大、各地发展不均衡，所以在网速上仍存在较大的提升空间。

在上述不愿具名的人士看来，即使基于CNNIC的网络速度报告，相比发达国家，我国在网速上并不占太大优势。“这与中国的具体国情有关。报告中提到的新加坡以60.39Mbps居首，瑞典和丹麦并列第二，这几个国家首先是经济发达，此外信息基础设施建设较为完善。同时，这前几名的国家有一个共同特点是国土面积较小、人口较少。”

而我国的特点是幅员辽阔、人口众多。人口众多意味着以同样的经费来建设满足1千万人联网的设施，最后的网速指标肯定会受到较大影响。幅员辽阔这个特点就意味着人均投入高。

“打一个较为极端的比方，如果在甘肃、青海、西藏这些地广人稀的地方实现‘村村通’，要铺设的光缆净长需以万公里计算，建设成本和维护成本极其高昂，但是这种大规模投资对全国平均网速提升并不太明显。尽管如此，这个工作也一定要做，我们的发展应尽量去照顾各个地区的情况。”上述不愿具名的人士说。

就如何提升我国网络水平，闫怀志认为，中国正在从网络大国向网络强国迈进。网络强国的要义不在于网速快慢的具体指标，而在于能够有力促进和保障我国社会经济的全方面发展。在这个过程中，应加强网络基础设施建设尤其是宽带建设，提升网络服务水平和服务质量，同时要坚守安全、自主、可控的原则。

“网络核心技术一定要自主、可控，从一个激光发射器到板卡交换芯片，再到网络体系架构乃至到整体成套设备的研发，都要符合这一原则。同时还应一步一个脚印形成通信行业完整的产业链，从而逐步提高我国的网速。”上述不具名人士强调。

（本版图片除标注外来源于网络）