

股票代码：600579

股票简称：天华院

公告编号：2018-071

青岛天华院化学工程股份有限公司

关于 KM 集团网络攻击事件的公告

本公司董事会及全体董事保证公告内容不存在虚假记载、误导性陈述或者重大遗漏，并对其内容的真实性、准确性和完整性承担个别及连带责任。

2018 年 12 月 21 日，本公司接本次重大资产重组交易对方 CNCE Global Holdings (Hong Kong) Co., Limited（中国化工装备环球控股（香港）有限公司）通知，标的资产 China National Chemical Equipment (Luxembourg) S.à r.l.（装备卢森堡）下属最终运营主体 KM 集团 IT 系统近期受到网络攻击，进而导致部分工厂产品生产、组装及交付延迟，对 KM 集团 2018 年 11 月、12 月经营业绩产生不利影响，相关具体情况如下：

一、网络攻击事件的具体情况

经 KM 集团管理团队确认，2018 年 11 月下旬 KM 集团遭到黑客入侵，本次网络攻击总计入侵了 349 个基于 windows 系统的 IT 管理系统，同时，备份服务器也遭到清除。网络攻击事件发生后，KM 集团立即启动应急预警状态，对约 170 个服务器进行了关闭或切换操作，以避免进一步入侵和感染。服务器和系统的关闭导致 KM 集团邮件系统、互联网连接以及与之有关的部分生产系统受到影响。

本次网络攻击导致 KM 集团子公司 KMT 慕尼黑工厂及其他五个相关生产组装点的工程加工、组装交付能力受到一定影响。产生影响的因素包括：①注塑设备板块的配件备件加工环节部分重要数据被加密；②由于服务器系统关闭，组件生产环节无法及时完成新订单信息和生产参数信息的下载，进而影响调试安装进度；③在调试安装环节，无法安装设备操作软件，进而影响产品交付进度。

网络攻击事件发生后，KM 集团迅速做出反应，主要采取了包括切断恶意程序传播路径、清除 KM 集团 IT 系统中可能留存的其他木马工具或休眠工具、聘请专业 IT 安全顾问等应对措施。在受攻击的 349 个系统中，优先恢复 60 个核心

系统，目前已恢复正常运行的系统包括 SAP、SAP 仓库管理系统、邮件系统、网络连接、结算系统等。

针对网络攻击事件 KM 集团正在积极采取措施恢复生产并提升生产经营系统安全性，核心系统预计将会在 2019 年 1 月初全部恢复，其余系统在 2019 年 1 月至 2 月全部恢复完成。KM 集团 IT 团队和安全顾问公司就被加密的数据进行恢复，同时采取措施提升备份数据服务器的安全性。伴随 IT 相关生产管理系统和数据的逐步恢复，KM 集团将采取积极有效的措施增加生产班次进行生产，加快组装调试和产品交付。

二、网络攻击事件对 KM 集团经营业绩的影响

根据 KM 集团管理团队预计，本次网络攻击事件预计导致 KM 集团 2018 年度产生的损失约 1,200 至 1,500 万欧元（税前），主要包括因网络攻击事件生产停滞期间相关机器设备的折旧、对应期间无法工作生产部门员工的工资、信息系统恢复支出等。同时，由于受到网络攻击的部分工厂延迟交货，该部分订单的经营业绩无法在 2018 年度确认，预计将导致 KM 集团 2018 年营业收入下降约 5,000 万欧元，占 KM 集团 2018 年度预计营业收入的比例约为 3.57%。

三、网络攻击事件对本次重大资产重组交易的影响

本次 KM 集团网络攻击事件为偶发性事件，不会对 KM 集团生产经营模式及其可持续性造成重大影响，KM 集团已采取措施尽快实现生产恢复并加快延迟订单的交付，同时进一步增强其网络系统安全。因此，本次 KM 集团网络攻击事件不会对本次重大资产重组产生实质性影响。

本公司将积极关注 KM 集团网络攻击事件进展，按照相关法律法规的要求及时履行公告义务，保护广大投资者的利益。

特此公告。

青島天华院化学工程股份有限公司董事会

2018 年 12 月 22 日