国盟信息安全通报

2020 年 4 月 13 日第 213 期

全国售后服务中心

国盟信息安全通报

（第 213 期）

国际信息安全学习联盟

2020 年 04 月 13 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 431 个，其中高危漏洞 207 个、中危漏洞 184 个、低危漏洞 40 个。漏洞平均分值为 6.67。本周收录的漏洞中，涉及 0day 漏洞 151 个（占 35%），其中互联网上出现“WordPress Nashvilleparent Themes 开放重定向漏洞、Joomla! com_fabrik 目录遍历漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3567 个，与上周（3354 个）环比增加 6%。

主要内容

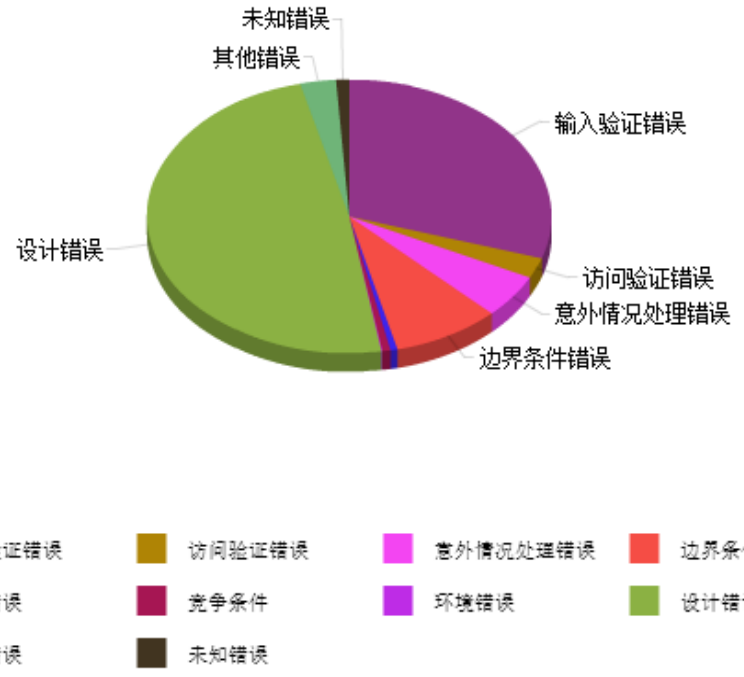
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

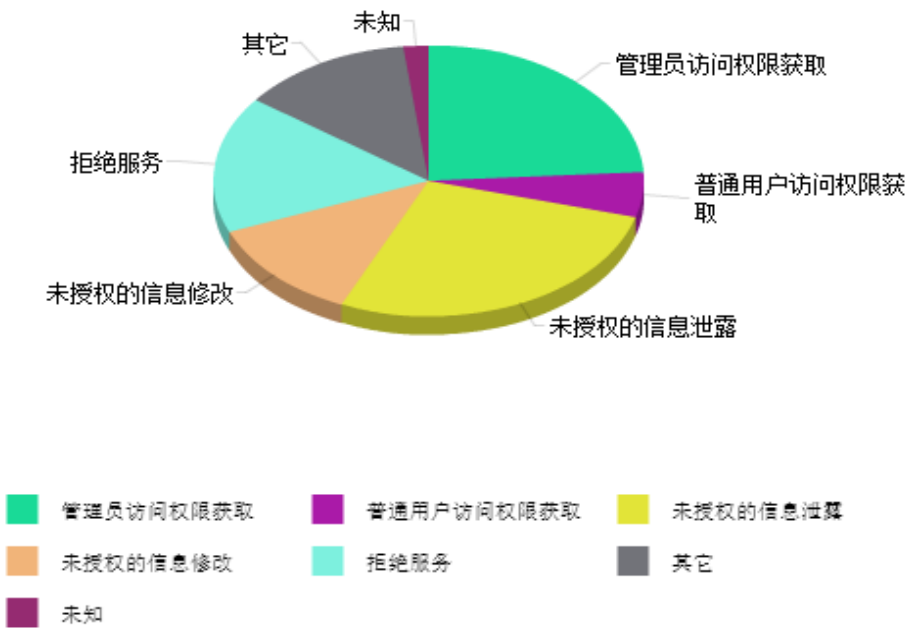
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 431 个，其中高危漏洞 207 个、中危漏洞 184 个、低危漏洞 40 个。漏洞平均分值为 6.67。本周收录的漏洞中，涉及 0day 漏洞 151 个（占 35%），其中互联网上出现“WordPress Nashvilleparent Themes 开放重定向漏洞、Joomla! com_fabrik 目录遍历漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3567 个，与上周（3354 个）环比增加 6%。

二、安全漏洞增长数量及种类分布情况

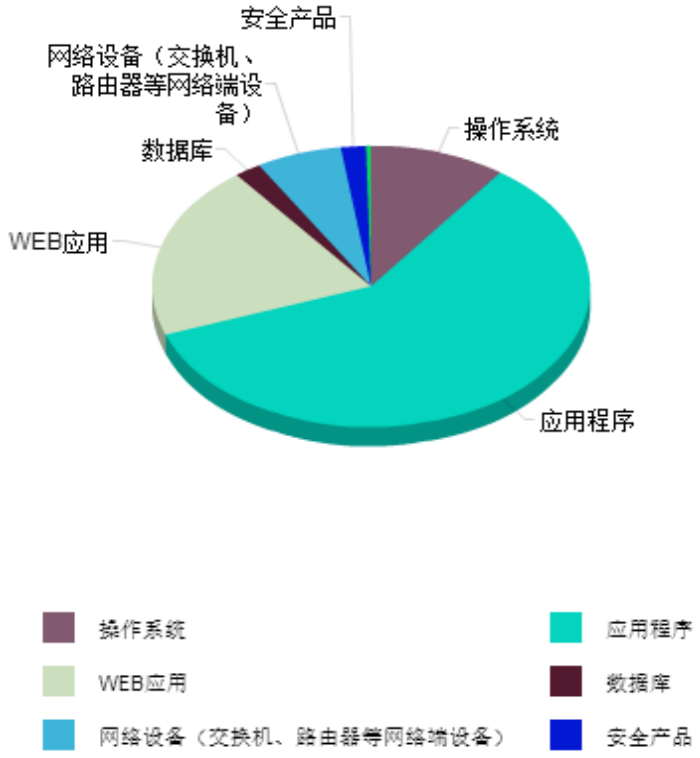
➢ 漏洞产生原因（2020 年 03 月 30 日—2020 年 04 月 12）



➢ 漏洞引发的威胁（2020 年 03 月 30 日—2020 年 04 月 12）



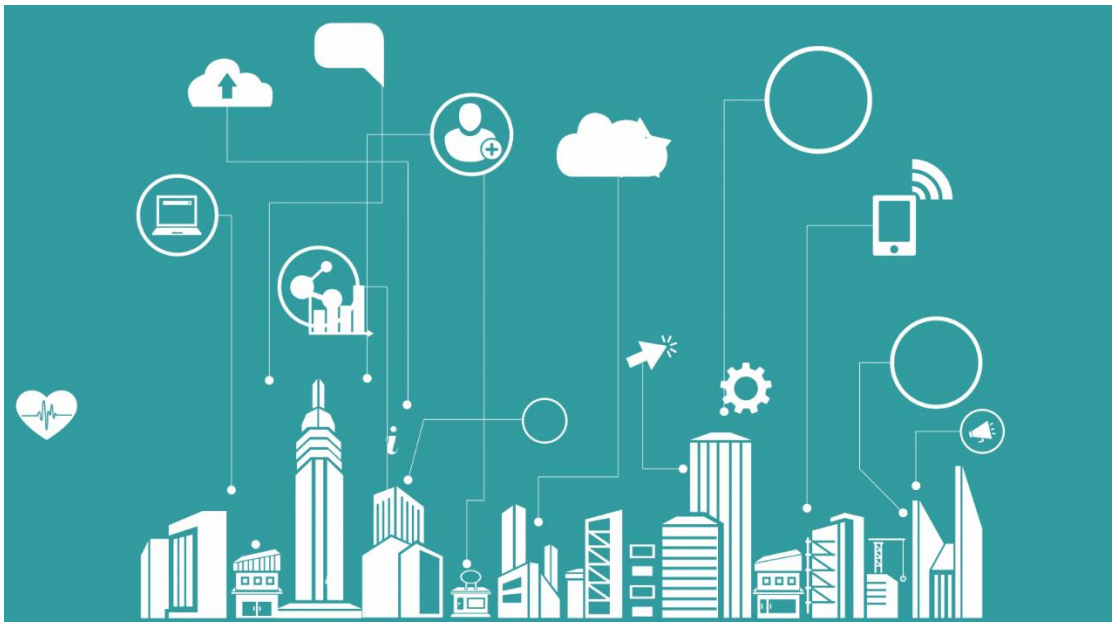
➢ 漏洞影响对象类型（2020 年 03 月 30 日—2020 年 04 月 12）



三、安全产业动态

➢ 工业互联网加速落地深耕 今年市场规模将超 3 万亿元

工业互联网领域“新政”和相关研究成果频频出炉：工业和信息化部近日发布《关于推动工业互联网加快发展的通知》（以下简称《通知》），要求推动工业互联网在更广范围、更深程度、更高水平上融合创新，培植壮大经济发展新动能。与此同时，中国信息通信研究院发布《工业互联网产业经济发展报告（2020 年）》，这是国内首次发布的工业互联网产业经济相关研究成果，为全面把握我国工业互联网产业经济发展态势、明确政策实施效果提供了重要参考。



业内人士称，当互联网进入下半场，工业互联网与 5G、大数据中心、人工智能等，一并构成了未来我国经济增长的新动能，也催生出产业链上下游数量巨大的投资机会。伴随着工业和信息化部《通知》的发布，工业互联网产业投资拉动和融合应用带动的外溢效应即将进一步释放，数万亿级的工业互联网市场也将迸发出新的生机和活力。

工业互联网“乘数效应”快速释放

当前，全球经济增长趋于放缓，我国“三期叠加”影响持续深化，经济下行压力加大。而以泛在互联、全面感知、智能优化、安全稳固为特征的工业互联网蓬勃发展，正在全球范围内加速颠覆制造模式、生产方式和组织形态，推动传统产业加快转型升级、新兴产业持续发展壮大。

工业和信息化部表示，当前以数字化、网络化、智能化为本质特征的第四次工业革命正

在兴起。工业互联网作为新一代信息技术与制造业深度融合的产物，通过对人、机、物的全面互联，构建起全要素、全产业链、全价值链全面连接的新型生产制造和服务体系，是数字化转型的实现途径，是实现新旧动能转换的关键力量。为抢抓新一轮科技革命和产业变革的重大历史机遇，世界主要国家和地区加强制造业数字化转型和工业互联网战略布局，全球领先企业积极行动，产业发展新格局正孕育形成。

近年来，我国工业互联网发展态势良好，有力提升了产业融合创新水平，有力加快了制造业数字化转型步伐，有力推动了实体经济高质量发展。工业互联网、5G、数据中心等数字基础设施日益成为新型基础设施的重要组成部分。这些高科技领域，既是基础设施，又是新兴产业，既有巨大的投资需求，又能撬动庞大的消费市场，乘数效应、边际效应显著。推动工业互联网加快发展，统筹疫情防控和经济社会发展，是缓解经济下行压力、兼顾短期刺激有效需求和长期增加有效供给的优先选择。

今年是工业互联网创新发展三年行动的收官之年。工业和信息化部指出，《通知》中各项举措的制定实施，既是立足当前巩固扩大工业互联网发展成效，培植壮大经济发展新动能的重要举措，更是面向未来为下一个五年发展奠定坚实基础的任务要求。

工业互联网市场规模将超 3 万亿

“在国家政策指导和有关各方共同努力下，我国工业互联网正由理念倡导加速走向落地深耕阶段，对经济社会发展的带动作用日益彰显。”中国信通院院长、工业互联网产业联盟理事长刘多如此表示。

刘多指出，工业互联网是新一代信息技术与工业经济深度融合的全新工业生态、关键基础设施和新型应用模式，将推动生产力跃升，促进生产关系变革。科学研判工业互联网产业经济发展态势，对企业运营、行业发展和政府决策具有重要的参考意义。

中国信通院政策与经济研究所所长辛勇飞介绍，测算表明，2018 年、2019 年我国工业互联网产业经济增加值规模分别为 1.42 万亿元、2.13 万亿元，占 GDP 比重分别为 1.5%、2.2%。预计 2020 年，我国工业互联网产业经济规模将达 3.1 万亿元，占 GDP 比重为 2.9%，同时可带动约 255 万个新增就业岗位。工业互联网产业经济核算包括核心产业及融合带动影响，随着工业互联网加速向各行业拓展，2019 年融合带动的经济影响占工业互联网产业经济比重已达 74.8%，工业互联网将成为国民经济中增长最为活跃的领域之一。

中国信通院信息化与工业化融合研究所数字化转型与智能制造研究部主任李铮表示，在当前这样一个特殊时期，制造业正在面临疫情带来的巨大挑战和冲击，而工业互联网作为整个工业体系与新一代信息技术深度融合的成果，作为整个工业数字化转型的赋能者和关键载

体，它在此次疫情防控和复工复产中发挥了重要作用。

李铮认为，工业互联网是企业数字化转型的一个关键路径，也是第四次工业革命的重要基石，它不仅仅是一个简单的网络，实际上是通过工业经济的全要素、全产业链、全价值链，全面链接所能够形成的重塑生产制造和服务体系的一个重要方向，它既有基础设施，也有形成的新兴业态和应用。

加快推进 5G 与工业互联网融合发展

记者注意到，工业和信息化部《通知》明确提出，“深入实施‘5G+工业互联网’512 工程”。那么，为何要推进 5G 与工业互联网融合发展？

专家指出，我国高度重视工业互联网和 5G 的发展。5G 是我国数字经济时代的重要引擎，在推进工业互联网发展过程中，5G 驱动作用不可小觑。

中国工程院院士邬贺铨认为，5G 将在工业互联网领域有很大的助力作用。他认为，5G 有三大应用场景：增强移动宽带、广覆盖大连接、超可靠低时延。消费互联网用到 5G，主要集中在增强移动宽带；广覆盖大连接和超可靠低时延的特性则是面向工业互联网的。邬贺铨预测，2035 年工业互联网会占 5G 整体收入的 80%。

根据工业和信息化部分析，当前我国工业互联网创新发展战略深入实施，5G 正式进入商用阶段，加快推动 5G 与工业互联网融合发展具有重要意义。

从工业互联网发展看，5G 是工业互联网的关键使能技术。5G 具有高速率大带宽、低时延高可靠、大连接广覆盖的技术特性，可有效满足工业业务苛刻的安全性、传输时延及可靠性要求，支撑工业互联网快速落地。特别是工厂内网改造方面，加快利用 5G 技术开展工业互联网内网改造，将有效促进工业互联网内网无线化、扁平化、IP 化发展，显著提升我国工业互联网产业发展水平。

从 5G 发展看，工业领域是 5G 的主要应用场景。5G 商用发展的重点是促进实体经济数字化、网络化、智能化转型升级，为各垂直行业和领域赋能赋智。当前，我国新型工业化发展步伐加快，工业领域已成为实体经济转型升级的关键领域。5G 在工业领域的成功应用将为 5G 发展开辟更为广阔的市场空间，有力拉动 5G 技术和产业进一步发展成熟，促进我国 5G 商用发展向更高水平迈进。

总体来看，我国 5G 与工业互联网融合发展仍处于起步阶段，但产业界探索步伐加快，积极性不断提升，已经具备良好的发展基础。

2019 年 11 月，工业和信息化部印发了《“5G+工业互联网”512 工程推进方案》，提出将重点提升“5G+工业互联网”融合发展的三个核心能力：一是提升“5G+工业互联网”技术

产业能力，二是提升“5G+工业互联网”创新应用能力，三是提升“5G+工业互联网”资源供给能力。

工业和信息化部指出，通过上述具体举措，加快推进 512 工程落地实施，夯实发展基础，提升产业能力，形成 5G 与工业互联网融合叠加、互促共进、倍增发展的创新态势。（来源：经济参考报）

➢ 新冠疫情对中国网络安全产业发展的影响

互联网在 2020 年新冠疫情处置中发挥了重大作用：民众通过互联网填报健康状况、获得疫情信息、购买日常用品、实现社区的协作，学校普遍开设了网络课堂，企业则纷纷开启远程工作模式。作为互联网安全保障的网络安全行业，肯定也受到新冠疫情影响，但是，用户行为和用户网络安全认知的变化，是过去多年想改变却未能成功的。新冠疫情给中国网络安全产业既带来威胁，也带来了产业升级的机会。

一、中国网络安全产业发展呈现阶段特征

根据中国信通院《中国网络安全产业白皮书 2019》，中国网络安全产业在过去六年获得了较快发展，行业总营收实现超过 15%的年复合增长，2019 年，行业总营收达到 630 亿人民币左右。总体看，中国网络安全产业具有如下特点。

一是“外甜内苦”，中国网络安全产业还在低水平发展。

外甜，是说网络安全事件非常吸引眼球。媒体于 2020 年 3 月披露的美国中央情报局对中国航空产业长达 11 年的 APT 攻击（APT-C-39）、2016 年美国大选攻击、2010 年“震网”

病毒攻击、针对沙特阿拉伯的 Shamoon 攻击等国家间的网络攻击事件，给习近平总书记“没有网络安全就没有国家安全”的论断做了完美的注解；台积电以及国内众多医院遭受勒索软件攻击，让更多人知道网络安全关乎生产安全；徐玉玉案、猖獗的网络电信诈骗，也让我们知道个人信息泄露会影响公民的生活安全。大众对网络安全的重视程度普遍提升，网络安全从业者的薪酬水平水涨船高，网络安全工程师成为热门职业。

内苦，是中国网络安全产业的规模还比较小。2019 年，整个网络安全产业的营收占全球 1000 多亿美金市场的不到 10%，与美国 500 亿美金以上的市场规模相比差了一个数量级，网络安全公司的盈利能力依然比较差。网络安全产业现在是劳动密集型高科技产业，而人力资源成本的提高进一步削弱了企业的盈利能力，很多中小型网络安全公司在为生存而奋斗，存在劣币驱逐良币现象，产业生态不够健康。

二是与美国网络安全产业的差别越来越大，“Copy to China”模式不再可行。

在过去的二十多年中，中国的网络安全产品研发大多采取跟随战略，反病毒软件、防火墙、下一代防火墙、IPS、IDS、WAF、扫描器等，基本上是把美国或以色列发明的产品在中国重新做一遍，但是，近几年，这条路越来越走不通。例如云安全代理（CASB）网关产品，Gartner 把它当作解决软件即服务（SaaS）安全的解决方案，也涌现出 Netscope、BitGlass 等厂商，但是，CASB 在中国几乎没有市场。在电子邮件安全网关（SEG）产品方面的情况也类似，这在国外是一个单独产品类别，不仅仅能防垃圾邮件，在对抗钓鱼攻击等高级威胁方面也非常重要，在美国有梭子鱼、MIMECAST、PROOFPRINT、INKY、趋势科技、FORCEPOINT 等多家厂商提供产品，但是，在中国，除了被绿盟科技收购的敏讯，几乎找不到 SEG 厂商，而敏讯也没有成为绿盟的主打产品，SEG 产品的销售额几乎可以忽略不计。

现在，已经不能简单把国外的网络安全产品照搬回国内，借鉴其防护思路、所采用的技术，而是需要针对国内的情况重新设计产品形态、商业模式和营销方案。

三是国家队和大型互联网企业大举进入网络安全领域，喜忧参半。

2019 年，国投智能成为美亚柏科的控股股东，中国电子 37.31 亿元人民币战略入股奇安信，中电科成为绿盟科技第一大股东，中电科收购南洋天融信 5.0065%股权，阿里云全资收购长亭科技和九州云腾布局企业级安全市场，腾讯也正式进入企业安全市场，更不用说做安全业务出身的 360 集团，在完成奇安信股权出售之后另起炉灶，重新打起 360 企业安全集团的大旗。

在中国的商业环境下，“国家队”和有钱、有人、有品牌的大型互联网公司更容易获得网络安全订单，大树之下不长草，安全创业公司想独立长大，会变得更加困难，成为大佬生

态圈的一员，会是很多创业企业的选择。这种情况有好也有坏，好的是创业企业的退出会变得更容易，坏处是大企业对市场的相对垄断以及官僚主义，可能会扼杀创新，而在网络安全行业，创新弥足珍贵。

四是创业企业团队成熟度较低，创业公司估值偏高，创业生态不够好。

相对于美国、以色列的网络安全创业公司，国内安全创业公司的创业者成熟度更低一些，偏技术和产品，企业运营和市场营销经验普遍缺乏，创新能力又比不上以色列安全创业公司，缺乏企业运营经验容易导致盲目扩张和资源的浪费。前几年，因为 3Q 大战、3B 大战所引发腾讯、百度、360、阿里巴巴等互联网公司在网络安全领域疯狂抢人、抢公司，把网络安全创业公司的估值推到不合理的高度，几年下来，多数创业公司的营收规模和盈利水平还无法匹配现在的估值水平，融资压力大，加上网络安全公司的退出周期比较长，导致风投难以退出，2018 年以后，专业的投资基金对网络安全公司依然感兴趣，但是，投资会比较谨慎。

五是网络安全合规依然是主要驱动力。

合规驱动，是中国和美国、欧盟都存在的现象。网络安全合规，其实就是要求组织在网络安全上按照有关法律法规把必须要做的事情做了，是从事某种业务所需要达到的网络安全法规的“及格线”。网络安全是攻与防的较量，但是，也有运气因素。网络安全做得不好的组织，也可能因为无人关注而没有发生安全事故，也有网络安全工作做得不错，却百密一疏，遇到顶尖高手的攻击而功亏一篑。不过，只是安全工作做得好的组织，发生事故的概率会低一些。

在安全防御效果类产品与合规类产品之间，国内的网络安全技术人员往往会看不起合规类产品，这是一种技术偏见。合规不能保证不出事故，但是，不合规，肯定更容易出事故。把合规类产品做得更好用、更有效果，是产业界应该追求的，要让自己的产品使客户在合规的基础上获得更好的防御效果。

二、新冠疫情对中国网络安全产业的影响

短期看，新冠疫情会给网络安全公司的现金流带来压力。

新冠疫情影响网络安全项目进度以及回款周期，从政府到企业的最高优先级都是处理疫情相关事务，各种人员流动管理措施使得拜访客户几乎不可能。网络安全建设项目延期，没有新的资金进来，但是，员工的工资要照发，公司的运作也不能停，网络安全公司现金流压力会变大。

对 2020 年全年业绩影响，主要看疫情能否在一季度平息。

考虑到每年的第一季度是网络安全企业的销售淡季，如果新冠疫情能在一季度末平息下

来，二季度社会全面复工的话，对网络安全企业 2020 年业绩的影响，应该不会很大。网络安全企业的客户多以政府和大型企业为主，网络安全支出在当年度的预算中已经确定，而这次受新冠疫情影响较大的广大中小企业恰恰不是网络安全公司的主要客户。如果新冠疫情到第二季度还无法彻底平息，甚至发生全球大爆发，可能会导致很多安全建设项目的取消或延迟到 2021 年进行，人力成本会成为网络安全企业维持运营的沉重负担，会有大问题。

三、新冠疫情给网络安全产业带来新的机会

首先是 SaaS 安全可能会兴起。

因为疫情所带来的人口流动的限制，各家企业纷纷开启远程办公模式，政府也开放了更多的在线服务，连大、中、小学也纷纷开始网课课堂。等疫情结束，大家可能发现远程工作其实也不错，如同 2003 年“非典”（SARS）疫情促进了中国电商行业的发展一样。有远程办公需求，就有远程办公的网络安全问题要解决，有远程教育，就有远程教育的网络安全、数据安全问题要解决。春节后，虚拟专用网络（VPN）厂商很忙，因为 VPN 是远程办公网络安全工具之一。各种 SaaS 服务被广泛接受后，SaaS 的安全也会成为一个问题，我们会面临和欧美同样的网络安全问题，这些都是给从事 SaaS 安全、零信任等解决方案公司的机会。

其次是网络安全在线服务/托管服务的机会。

因为各种原因，中国的客户更习惯于网络安全厂商提供面对面服务，但是，面对面服务的人员利用效率比较低，且不说异地长途旅行的时间开销，单是在北京这样的城市，5 分钟就能解决问题却需要 3 小时往返在路上。由于疫情所造成的出行限制，已经逼迫部分客户开放远程安全运维端口。疫情过后，他们或许会发现，其实是有技术和管理手段把远程运维的风险降低到可接受的程度：堡垒机、远程桌面、安全运维审计系统本身就是干这个用的！远程运维情况下，自己能得到更快的响应以及更高水平专家的服务。对网络安全企业来讲，这是提高人员复用率，进行运维知识积累，形成运维知识库，提高运维自动化水平的机会，可以提高企业运营效率，降低运营成本。

再次，数据安全在新冠疫情后被进一步重视。

大数据在新冠疫情处置过程中发挥了很大作用，例如运营商通过大数据提供公民到访城市的信息，支付宝的“健康码”可以利用大数据自动得出某人是否具有传染风险的结论。在杭州，如果不展示支付宝健康码，几乎不可能出门。用数据标示感染风险等应用，也肯定会引发对大数据滥用与用户隐私保护的担忧。匆忙上线的信息系统也可能存在安全漏洞，疫情期间收集的大量用户信息肯定也会成为黑客攻击的目标，存在泄露用户个人信息的可能。数据安全在疫情过后肯定会引起关注，这对从事数据安全、用户隐私保护产品或服务的公司都

是机会。

最后，新冠疫情后网络安全产业也会吃到红利。

新冠疫情之后，我国应该对灾难应急响应体系做一次升级，为下一次类似甚至更严重疫情爆发做好准备。大范围、长时间的隔离肯定会是假设前提，更多的线上服务、线上协同，甚至无人系统提供服务，都可能变成应对手段，而我们肯定要为此准备好网络安全防护方案，无人车、机器人、无人工厂、无人机等物联网世界的安全，都是要解决的问题，而远程的安全运维服务，将会变成网络安全服务的必选项。

四、抓住机遇，实现网络安全产业升级

新冠疫情给我国网络安全产业既带来生存的压力，也带来产业转型升级的契机，需要抓住这次机遇，实现网络安全服务化、云化、智能化、自动化、人性化，实现安全合规与安全防护效果双驱动。

实现网络安全产业转型升级，需要有对网络安全具有深刻理解，有理想与抱负的企业家，带领企业脚踏实地用创新的思路开发出好的产品，培养优秀的安全服务人员，摆正技术与销售的关系，避免过度技术，管好现金流，通过精细化运营控制经营成本，解决用户问题；需要有远见、有耐心的投资者，通过资本的力量扶持大量的创新创业者，通过收购与兼并、IPO 等在投资人挣钱的同时让创业者有回报；需要教育机构为产业培养大批的网络安全人才；需要在网络安全的法律法规、网络安全的考评标准方面，跟上技术与商业模式进步的节奏；需要有对网络安全清晰认知的客户，共同努力营造健康的网络空间安全产业生态。（来源：中国信息安全》杂志 2020 年第 3 期）

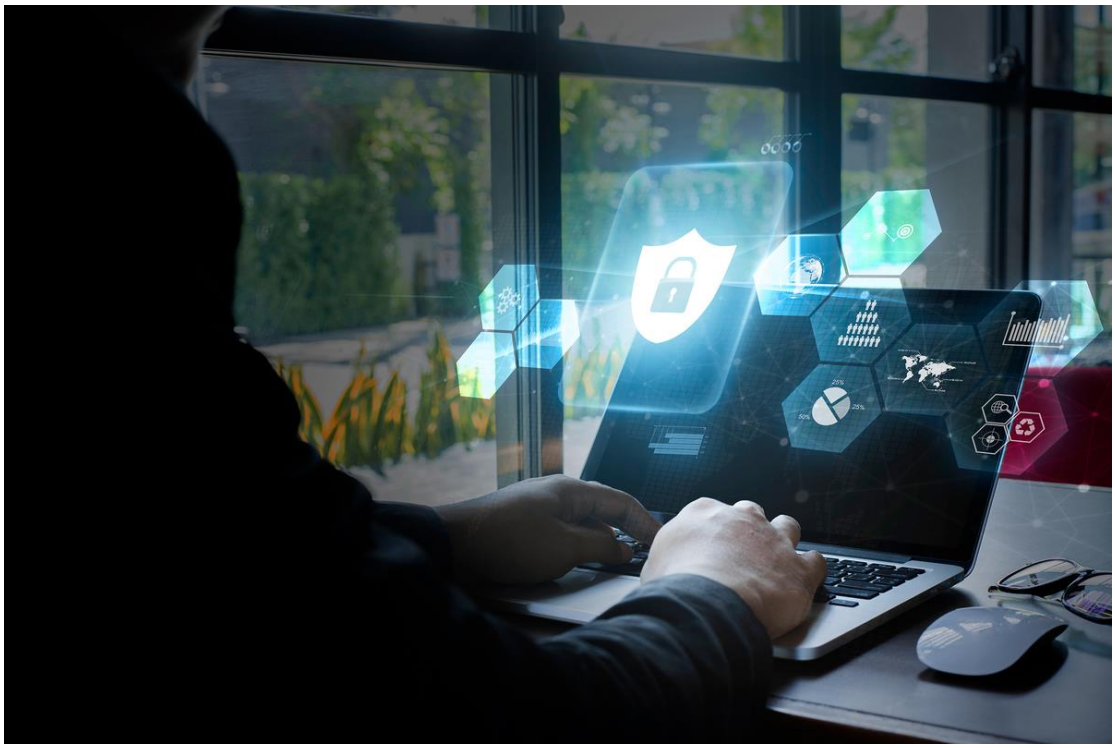
➢ 我国关键信息基础设施网络安全应急响应的法律保障

2020 年，面对严重威胁生命安全的疫情冲击，我国 26 个省、市、自治区启动重大突发公共卫生事件一级响应，国家应急管理基础能力和治理能力接受检验。世界卫生组织专家在 2020 年 2 月 24 日世卫组织-中国冠状病毒病联合专家考察组新闻发布会上坦诚，“我们需要审视现有体系，坦率地说，没有任何一个体系能做到及时响应”。根据《网络安全法》第 57 条的规定，网络安全事件在符合“突发事件”的构成要件后，将转化或“升级”为突发事件，从而同时适用《突发事件应对法》等法律的处置。因此，网络安全事件与公共安全事件在突发事件应对上有普遍性的一面，本次重大突发公共卫生事件的响应和处置为关键信息基础设

施网络安全事件应急响应触动思考。

一、关键信息基础设施网络安全应急响应法律规制的必要性

全球数字化转型浪潮之下，人工智能、区块链、5G 等新一代信息技术不断催生新业态新产业新模式，传统关键信息基础设施的“边界性”逐渐模糊，新型网络安全风险与威胁不断衍生与演化。近年来，网络攻击方式、手段的多样性和严重性不断刷新各国对网络安全态势的认知，网络空间安全的不稳定性和不确定性愈加凸显，以往以关键信息基础设施静态识别为核心的保护观念在面对全新威胁态势时挑战严峻。如何健全完善关键信息基础设施网络安全监测预警响应机制，提升国家层面的网络安全态势感知、事件分析、追踪溯源以及遭受攻击后的快速恢复能力，实践中有效应对国家级、有组织的高智能攻击，针对网络攻击实施精准打击，同时允许有条件的攻击反制，为公共卫生安全等其他突发事件提供重点保障和支持，是各国关键信息基础设施保护的重中之重。我国《国家突发事件应急体系建设“十三五”规划》即明确提出,提高关键信息基础设施的风险防控能力，保障金融、电力、通信、交通等基础性行业业务系统安全平稳运行，同时强调要充分利用互联网、大数据、智能辅助决策等新技术，在应急管理相关信息化系统中推进应急预案数字化应用。2020 年中央网信办《关于做好个人信息保护利用大数据支撑联防联控工作的通知》也直接提出借助大数据等各类网络信息技术为疫情防控应急响应提供必要的技术支撑。



事实上，关键信息基础设施立法保护已成为全球“显学”，鉴于地缘政治、经济发展、立法模式等方面的天然差异，各国关键信息基础设施的立法思路及侧重有所不同，但无一不

聚焦网络安全应急响应。整体上，各国普遍承认 100%安全目标不可实现，重在以“风险（管控）”、“预判（感知）”和“攻击（假想）”为基础，重点构建特定关键信息基础设施范畴的网络监测预警、网络安全威胁情报信息共享、网络安全评估检测、供应链安全审查、网络安全事件应急处置、公私合作和国际合作等要素的网络安全应急响应保障体系。此外，随着贸易全球化趋势不断强化，共同制定关键信息基础设施网络安全应急响应的国际规范，保障全球关键信息基础设施的整体安全性和可靠性，也是国际关键信息基础设施保护的关注重点。

二、我国关键信息基础设施网络安全应急响应的法制化

在我国，以《网络安全法》为核心的关键信息基础设施网络安全应急响应法律保障体系建设正在加速推进。2007 年《突发事件应对法》、2016 年《网络安全法》、2006 年国务院《国家突发公共事件总体应急预案》、2013 年国务院《突发事件应急预案管理办法》、2017 年中央网信办《国家网络安全事件应急预案》等现行有效的法律法规共同构筑了关键信息基础设施网络安全应急响应法律保障基本体系。《国家网络空间安全战略》明确要求完善网络安全监测预警和网络安全重大事件应急处置机制。《网络安全法》将监测预警与应急处置措施制度化、法制化，设第五章专章规定了网络安全监测预警、信息通报和应急处置制度，重点强化关键信息基础设施领域的应急响应制度，同时第 57 条有效衔接《突发事件应对法》、《安全生产法》等法律、行政法规的处置规定。2017 年 1 月，作为国家层面针对网络安全事件适用的综合应急预案，中央网信办正式发布《国家网络安全事件应急预案》。以《突发事件应对法》、《网络安全法》等为依据，行业领域的相关部门、地方政府等也制定了相应监管范围的网络安全应急预案，如《银行业重要信息系统突发事件应急管理规范（试行）》《证券期货业网络与信息安全事件应急预案》《公共互联网网络安全突发事件应急预案》《工业控制系统信息安全事件应急管理工作指南》《上海市网络安全事件应急预案》等。

从实践来看，《网络安全法》实施以来，面向勒索病毒攻击、DDoS 攻击、Web 站点攻击等当前主要的网络攻击方式，我国深入推进网络安全等级保护，强化关键信息基础设施摸底排查、安全防护和执法检查，从实战出发落实国家重大网络安全保卫任务,覆盖国家、行业领域、地方政府、网络运营者的多级监测预警应急响应机制基本建立。从本次疫情响应来借鉴思考，关键信息基础设施的国家应急意愿与具体行业、领域和地方的应急能力是否一致需要进行重新验视，国家层面的综合应急能力如何穿透、赋能到具体的关键信息基础设施运营者，也应从利益共同体和整体价值上重新整合考虑。

此外，2017 年以来，《关键信息基础设施保护条例（征求意见稿）》《网络安全等级保护条例（征求意见稿）》《网络安全漏洞管理规定（征求意见稿）》《网络安全威胁信息发布管理

办法（征求意见稿）》等相继向社会公开征求意见，进一步细化了《网络安全法》关键信息基础设施网络安全应急响应、网络安全等级保护、网络安全漏洞发现与披露、威胁信息发布等方面的规定。这些尚处于综合研判、统筹调整阶段的《网络安全法》下位法是关键信息基础设施网络安全应急响应不可缺失的组成部分和制度支撑，如其中涉及的关键信息基础设施识别与认定、网络安全漏洞发现与公布、境内外网络安全威胁态势感知、关键信息基础设施供应链安全保障、网络安全信息共享、安全漏洞信息出口管制机制等问题，重要性自不待言。

三、我国关键信息基础设施网络安全应急响应法律制度的完善

为有效应对网络空间安全威胁和风险，关键信息基础设施网络安全应急响应法律体系必须以发现、消除网络安全威胁和风险，提升恢复能力为轴心，“发现、消除、恢复”金三角作为对包括公共卫生事件、网络安全事件等混合与叠加的动态“全风险环境”的提升完善。

具体来说，“发现”包括网络安全漏洞的掌控、攻防演练、网络安全威胁和风险的实时全面共享、侦查、监测预警和供应链安全等。“发现”能力的提升意味着需从法律上对溯源的触发条件、电子证据固定与提取等内容进行发展与规范。以跨境威胁行为发现来说，《网络安全法》第 5 条和第 75 条规定为跨境数据取证确立了国家立法基础，执法机关仍需面临跨境数据取证实际取证技术能力的现实考验。“消除”包括及时动态研判处置网络攻击，实施精准化解、消除和阻断的同时允许有条件的攻击反制，消除能力的实现需要从法律上对反制的必要性和充分性进行正当化论证，以主动防御来说，这个概念的边界在网络安全管理和法律层面的争议已经持续多年，立法上启动后将引发不可预测性的内外部后果，其使用条件应周延论证。“恢复”侧重网络安全态势感知和网络攻击之后的应对恢复，确保核心功能正常运转。事实上，“恢复”并不仅单指关键信息基础设施功能的修复与重启，而应更加关注关键信息基础设施核心功能的持续运行。通过构筑、有效实施面向“全风险”的“全能力”，保护有关各方的合法权益，提升各方对社会稳定和国家安全的信心。（来源：公安部第三研究所 黄道丽）

➢ 数据安全也要加把“保护锁”

最近，两起有关数据安全的事件引发关注。工信部近日就新浪微博 App（手机应用程序）数据泄露问题，对其相关负责人进行问询约谈。新浪微博回应称，已采取了升级接口安全策略等措施，后续将落实企业数据安全主体责任，切实做好用户个人信息保护工作。此前，为

线上商户提供营销服务的微盟发生业务数据丢失事故，给企业和商户造成严重影响。数据安全保护事关每位公民的合法权益，也事关企业发展和经济社会大局。在大数据时代，如何增强人们的数据“安全感”？

谁动了“你”的数据？

当用户注册某个手机软件时，会弹出要求用户授权通讯录、麦克风、地理位置各类信息权限的条款；在街边或商场的促销活动上，商家招揽顾客扫码免费领取奖品；在商场等公共场所，看到来历不明的免费无线网络，一些人会不加考虑地连接上网……日常生活中，人们经常遇见这样的场景。不经意间，个人的数据信息面临着被直接或间接“窃取”的风险。

随着互联网的迅速普及和信息化的深入发展，各种数据化信息被快速生产、收集、储存、处理和利用，大数据时代随之来临。

当今社会，数据被视为一种新型资源。通过对收集的用户数据进行深入分析和挖掘，企业能根据客户的地域、类别、喜好、社交需求等个人信息，综合判断用户的消费需求，更加精准地“推销”产品，谋划产业布局。

大数据在带来新机遇的同时，也带来了新挑战，数据泄露、数据滥用等安全风险突出，隐患不小。一旦数据泄露或者被滥用，骚扰电话、网络诈骗等也可以由“误打误撞”变为“精准定制”。

守住数据安全“红线”

“数据安全问题处理得好坏，直接影响到个人隐私甚至社会秩序和国家利益，这是数字经济发展道路上必须面对的挑战。”北京邮电大学网络空间安全学院教授辛阳指出。

在大数据时代，信息所具有的商业价值日渐成为企业的核心竞争力，越来越多的企业投

入巨资收集、整理和挖掘信息。如何平衡个人信息保护与产业发展间的关系，成为当下亟待解决的问题。

2019 年 1 月至 12 月，中央网信办、工信部、公安部、市场监管总局四部门在全国范围组织开展 App 违法违规收集使用个人信息专项治理。2019 年 12 月 30 日，四部门联合印发《App 违法违规收集使用个人信息行为认定方法》，将 31 种违法违规收集使用个人信息行为进行了分类认定，为移动互联网企业划定用户数据安全保护的“红线”。

业内人士指出，大数据采集要遵循三个原则：合法原则，即不得窃取或者以其他非法方式获取个人信息；正当原则，即不得以欺骗、误导、强迫、违约等方式收集个人信息；必要原则，即满足信息主体授权目的所需的最少个人信息类型和数量。

合力强化数据“安全感”

近日，工业和信息化部关于推动 5G 加快发展的通知，强调进一步强化 5G 网络数据安全保护，指出要围绕典型应用场景，健全完善数据安全管理制度与标准规范；要合理划分网络运营商、行业服务提供商等各方数据安全和用户个人信息保护责任等。

5G 时代到来，数据安全保护面临着更大的挑战。各方应加强合力，让非法收集、滥用数据的“灰色空间”越来越小，让用户的数据安全感越来越实。

近年来，中国不断加快相关法律制度建设。2017 年 6 月 1 日实施的网络安全法，对个人信息保护提出专门要求；2018 年 5 月 1 日，国家标准《信息安全技术个人信息安全规范》正式实施；2019 年 5 月，国家网信办发布《数据安全管理办法（征求意见稿）》。

此外，针对个人信息数据安全，国家和地方层面上的专向整治活动力度不小，为数据安全上紧“保护锁”。2020 年初，浙江警方针对全省互联网企业涉个人信息数据安全的专项整治工作拉开序幕，此次活动将贯穿全年，将有效打击整治与个人信息安全相关的违法犯罪，加强互联网企业的数据安全保护，规范互联网企业涉个人信息经营行为。

业内人士指出，对互联网企业而言，要强化法治思维，落实法律规范，守住法律底线，这是落实大数据发展战略、推动企业数据类型业务有序发展的重要保障。平台方应通过用户协议或隐私协议等方式，明确告知用户收集信息的具体内容和目的，坚持“最少必要”的原则。对用户而言，每个人都要为个人信息把关，养成安全使用手机软件的习惯，当发现个人信息被泄露时，要勇于拿起法律武器维护自身合法权益。（来源：人民日报）

四、政府之声

➢ 中共中央国务院发布关于构建更加完善的要素市场化配置体制机制的意见

2020 年 4 月 9 日，中共中央国务院公布了《关于构建更加完善的要素市场化配置体制机制的意见》（以下简称《意见》），明确提出“加快培育数据要素市场”。推进数据要素配置模式探索，破除数据自由流动的体制机制障碍，深化数据要素价格改革，加快建立健全数据治理体系，充分发挥数据这一新型要素对其他要素效率的倍增作用，培育发展数据要素市场，对释放数据红利推动数字经济高质量发展具有十分重要的战略意义。


中华人民共和国中央人民政府
www.gov.cn
简 | 繁 | EN | 注册 |
国务院 总理 新闻 政策 互动 服务 数据 国情 国家政务服务平台
首页 > 政策 > 中央有关文件
收藏 留言
中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见
2020-04-09 19:00 来源：新华社
【字体：大 中 小】 打印
新华社北京4月9日电
中共中央 国务院
关于构建更加完善的要素市场化配置体制机制的意见
（2020年3月30日）
完善要素市场化配置是建设统一开放、竞争有序市场体系的内在要求，是坚持和完善社会主义基本经济制度、加快完善社会主义市场经济体制的重要内容。为深化要素市场化配置改革，促进要素自主有序流动，提高要素配置效率，进一步激发全社会创造力和市场活力，推动经济发展质量变革、效率变革、动力变革，现就构建更加完善的要素市场化配置体制机制提出如下

一、《意见》是发展数据要素市场体系的重要举措

《意见》是落实国家战略部署提升国家数字竞争力的关键一环，对培育数据要素市场提出了全局性的部署要求，为下一步推动培育数据要素市场提供了根本遵循。

《意见》有利于实现数字经济高质量发展。党中央、国务院高度重视大数据在推动数字经济发展中的作用。习近平总书记在十九届中央政治局第二次集体学习中提出要构建以数据为关键要素的数字经济。党的十九届四中全会通过的《中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定》（以下简称《决定》）明确指出“健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、

按贡献决定报酬的机制”，首次提出将“数据”作为生产要素参与分配，这为数据赋予了新的历史使命。国务院印发《促进大数据发展行动纲要》，要求全面推进我国大数据发展和应用，加快建设数据强国，释放技术红利、制度红利和创新红利。《意见》积极对标国家战略要求，对建立数据要素市场提出明确要求，旨在破除数据价值挖潜的体制机制障碍，凝聚各方协同发掘数据价值，推动数字经济高质量发展。

《意见》有利于重塑国际竞争新优势。数据在全球经济运行中的重要性日益显现，世界各国积极布局数字经济发展。随着《美国联邦大数据研发战略计划》《欧洲数据战略》的部署实施，日美欧跨境数据流通圈逐步形成，全球数据竞争格局日趋紧张复杂，促使数字经济国际竞争愈发激烈。数据作为一种新型生产要素，是继土地、劳动力、资本之后，全球数字经济竞争的新赛道。正如习近平总书记 2013 年视察中国科学院时就曾指出：“大数据是工业社会的‘自由’资源，谁掌握了数据，谁就掌握了主动权。”不可否认，数据正成为新时代体现国家综合实力、重塑国际竞争优势的关键要素。《意见》围绕推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护等方面提出指导意见，为数据要素市场培育指明了方向。

《意见》有利于释放数字化转型潜力。数据不仅是数字化转型的关键要素，更是数字化转型的新动能。随着数字经济的发展，以大数据为代表的数据资源向生产要素的形态演进，数据已和其他要素一起融入经济价值创造过程，对生产力发展产生广泛影响。通过制度设计合理配置数据资源，让各数据利益攸关方充分发挥作用，构建智能时代的新型数据生产关系，可以不断提升利用数据创造价值的能力。数据生产要素属性的提升，关系经济增长的长期动力，关系国家发展未来。世界各国都把推进经济数字化作为创新发展的重要动能，在前沿技术研发、数据开放共享、隐私安全保护、人才培养等方面做出前瞻性布局。推动实体经济和数字经济融合发展，推动制造业加速向数字化、网络化、智能化发展，运用大数据提升国家治理现代化水平，提高感知、预测、防范风险的能力。《意见》对数据要素市场培育提出要求，不仅是落实党中央将数据作为生产要素的部署安排，提升国际竞争优势的关键举措，更是以数字化带动制造业全面升级、实现国家治理现代化的现实需要。

二、《意见》明确了培育数据要素市场的“着力点”

《意见》提出了培育数据要素市场的主要内容，指明了数据治理体系建设方向，为全面释放数据价值奠定良好基础。

政府数据开放共享是构建数据要素市场的探路者。《意见》明确提出以数据共享责任清单为抓手，加快推动政府共享，研究建立公共数据开放和流动的制度规范。近年来，在公共

数据开放共享等文件的推动下，我国公共数据开放共享取得积极进展。但是开放数据质量不高、共享意愿不强的现象依然存在，政府、企业、个人不同主体获取数据的困难依然存在，致使经济社会运行的各个领域未能得到全面的数据支持。加快政府数据开放共享，政府先行，让政府数据像水一样，随需而动，滋养各个领域，可以为企业和个人数据要素市场化有序流动提供良好经验。

释放社会数据资源价值是构建数据要素市场的原动力。《意见》明确指出支持重点领域数据开发利用，推动数据密集型行业数据采集标准化，发展数字经济新产业、新业态和新模式。当前，我国数据规模庞大，但很多行业的数据处于睡眠状态，其潜在的价值尚未释放，同时大量数据的存储维护也产生了一定的成本。人工智能、可穿戴设备、车联网、物联网等数据密集型领域标准不一，增加了数据共享互认的难度。推动相关行业数据采集标准化，探索数据规范化开发利用，是推动数据价值释放的基本前提，也是数据要素市场化发展的重中之重。

数据资源整合和安全保护是构建数据要素市场的生命线。《意见》提出要建立统一规范的数据管理制度，研究根据数据性质完善产权性质，制定数据隐私保护制度和安全审查制度，完善数据分类分级安全保护制度。各地对释放数据红利，激发创新活力的愿望十分迫切，但存在数据管理权责不清、资源运营无法可依、收益分配无章可循、信息安全和个人隐私保护力度不够等问题，成为阻碍数据市场化流通的一大障碍。提升数据管理能力，理清数据产权体系，开展数据分类分级，结合不同数据的属性和安全防护要求，加大数据安全保护力度，是数据要素市场得以有效运行的必要选择。

三、联合多方协力做好《意见》推进落实

建立数据要素市场体系是一项复杂的系统工程，《意见》是否能宣贯落实到位，是否能探索出一套符合中国国情的数据要素市场体系，对数据要素市场培育至关重要。前期，赛迪对公共数据资源配置模式、价格形成机制、管理制度等开发利用重点问题开展了深入研究，并支撑了公共数据资源开发利用相关工作。下一步，我们将积极与不同行业企业共同协作，不断提升数据要素市场培育方面的服务能力，为数据要素市场体系建设提供有力支撑。

一是加强服务能力建设。针对数据资产评估、数据交易定价、数据流通管理、数据安全保障、数据治理体系、数据治理绩效评估等关键问题，联合产学研不同优势资源，以研究咨询、评测认证为重点，以数据要素市场基础理论研究为牵引，面向行业主管部门、数据交易平台、数据运营公司等不同行业主体，为数据要素市场体系构建提供全方位整体解决方案。

二是加大行业宣贯力度。充分利用赛迪的媒体、联盟、协会资源，加大对数据要素市场

培育的宣传力度，及时向社会广泛传播数据要素市场培育的政策重点、实践案例、专家观点等热点，积极营造全社会协同建设数据要素市场体系的文化氛围，让参与各方深刻认识到数据要素市场的重要性，积极参与到构建数据要素市场体系工作中来。

三是做好政策实施推广。利用联盟、协会桥梁纽带作用，定期组织数据要素市场体系相关活动，促进各级行业主管部门、不同行业领域、高等院校、科研事业单位及企业等各类机构间交流合作。发挥赛迪培训基地的作用，利用各种渠道加大数据要素市场体系人才培养。为各级行业主管部门和有关企业做好数据要素市场化咨询服务，推动数据要素市场化顺利发展，促进数据价值有效释放。（来源：中国政府网）

- **中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见**
- **全文：**http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm

➢ 工信部公开征求《网络数据安全标准体系建设指南》（征求意见稿）的意见

2020 年 4 月 10 日，工业和信息化部为落实《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律法规要求，有效提升电信和互联网行业网络数据安全保护能力，充分发挥标准在保障网络数据安全、推动行业健康有序发展中的引领和支撑作用，助力数字经济高质量发展，有关单位编制完成了《网络数据安全标准体系建设指南》（征求意见稿）及编制说明（见附件 1、2）。


中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

邮箱登录 | 移动版网站 | 工信微报 | RSS订阅

统一搜索

看新闻 找文件 查办事 提意见 查数据 要投诉

工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据 专题专栏 疫情防控专题

首页 > 政务公开 > 文件公示 > 正文

公开征求对《网络数据安全标准体系建设指南》（征求意见稿）的意见

发布时间：2020-04-10 来源：科技司 分享：

为落实《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律法规要求，有效提升电信和互联网行业网络数据安全保护能力，充分发挥标准在保障网络数据安全、推动行业健康有序发展中的引领和支撑作用，助力数字经济高质量发展，有关单位编制完成了《网络数据安全标准体系建设指南》（征求意见稿）及编制说明（见附件1、2）。

为进一步听取社会各界意见，现予以公示，公示日期截止2020年5月9日。如有意见或建议，请在公示期间填写《公示意见反馈信息表》（见附件3）并反馈至工业和信息化部科技司，电子邮件发送至KJBZ@miit.gov.cn（邮件主题注明：网络数据安全标准体系建设指南公示反馈）。

地址：北京市西长安街13号 工业和信息化部科技司标准处
邮编：100846

为进一步听取社会各界意见，现予以公示，公示日期截止 2020 年 5 月 9 日。（来源：工业和信息化部）

- **《网络数据安全标准体系建设指南》（征求意见稿）**
- **全文：**http://www.miit.gov.cn/n1146295/n7281310/c7858148/content.html

➢ 市场监管总局国家密码管理局关于开展商用密码检测认证工作的实施意见

2020 年 3 月 31 日，国家市场监督管理总局网站发布《市场监管总局 国家密码管理局关于开展商用密码检测认证工作的实施意见》。

《实施意见》提出，商用密码检测认证工作坚持“统一管理、共同实施、规范有序、保障安全”的基本原则。市场监管总局、国家密码管理局根据部门职责，加强检测认证工作的组织实施、监督管理和结果采信，营造有利于商用密码发展的良好市场环境。商用密码认证目录由市场监管总局、国家密码管理局共同发布，商用密码认证规则由市场监管总局发布。市场监管总局、国家密码管理局联合组建商用密码认证技术委员会，协调解决认证实施过程中出现的技术问题，为管理部门提供技术支撑、提出工作建议等。

《实施意见》明确了认证实施工作的六项要求。商用密码认证机构应当符合有关行政法规、规章规定的基本条件，具备从事商用密码认证活动的专业能力，并经市场监管总局征求国家密码管理局意见后批准取得资质。商用密码认证机构应当委托依法取得商用密码检测相关资质的检测机构开展与认证相关的检测活动，并明确各自权利义务和法律责任。商用密码检测、认证机构应当依照法律、行政法规的规定和商用密码检测认证技术规范、规则开展商用密码检测认证，并建立可追溯工作机制对检测认证全过程完整记录并归档留存。商用密码认证机构应当公开认证收费标准、认证证书有效、暂停、注销或者撤销的状态等信息，接受社会的监督和查询。商用密码认证机构应当按照有关规定报送商用密码认证实施情况及认证证书信息。商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的国家秘密和商业秘密承担保密义务。

《实施意见》要求，市场监管部门会同密码管理部门对商用密码检测、认证机构及其活动实施监督管理，发现违法行为的，依法予以处罚。认证委托人对检测、认证机构的检测认证工作和检测认证决定有异议的，可以向作出决定的检测、认证机构提出申诉。对检测、认证机构处理结果仍有异议的，可以向市场监管部门或密码管理部门投诉。（来源：国家密码管理

局）

- **国家市场监管总局 国家密码管理局关于开展商用密码检测认证工作的实施意见**
- **全文：**http://sca.gov.cn/sca/xwdt/2020-03/31/content_1060707.shtml

➢ 最高检发布打击网络犯罪指导性案例 加强网络风险防控

2020 年 4 月 8 日，最高人民检察院召开新闻发布会以打击网络犯罪为主题发布了第十八批指导性案例。据通报，2018 年至 2019 年,检察机关共批准逮捕网络犯罪嫌疑人 89167 人,提起公诉 105658 人,较前两年分别上升 78.8%和 95.1%。为保证重大疑难案件顺利办理,2018 年以来,最高检先后挂牌督办社会广泛关注的电信网络诈骗案件和假借“金融创新”“互联网+”名义实施金融诈骗案件共 35 件。

此次，最高检第十八批指导性案例包括张凯闵等 52 人电信网络诈骗案,叶源星、张剑秋提供侵入计算机信息系统程序、谭房妹非法获取计算机信息系统数据案以及姚晓杰等 11 人破坏计算机信息系统案等。最高检第一检察厅厅长苗生明表示,下一步,检察机关将修改完善《检察机关办理电信网络诈骗和侵犯公民个人信息案件指引》,对网络赌博犯罪案件的法律适用进行专题分析研判。同时,强化与有关单位在网络犯罪追赃挽损上的协同作战,最大限度挽回受害群众损失。（来源：最高人民检察院）

- **最高人民检察院发布第十八批指导性案例**
- **全文：**https://www.spp.gov.cn/spp/xwfbh/wsfbh/202004/t20200408_458230.shtml

五、本期重要漏洞实例

➢ Microsoft Internet Explorer 脚本引擎远程代码执行漏洞

发布日期：2020-03-30
更新日期：2020-03-30
受影响系统：
Microsoft Internet Explorer 11
描述：

CVE(CAN) ID: CVE-2020-0832
Microsoft Internet Explorer（IE）是美国微软（Microsoft）公司的一款 Windows 操作系统附带的 Web 浏览器。
Microsoft IE 11 中脚本引擎处理内存对象的方式存在远程代码执行漏洞。攻击者可利用该漏洞在当前用户的上下文中执行任意代码，破坏内存。
链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0832
建议：

厂商补丁：
Microsoft
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0832

➢ SonicWall SMA1000 HTTP Extraweb 拒绝服务漏洞

发布日期：2020-03-31
更新日期：2020-03-31
受影响系统：
SonicWall SMA1000 <=12.1.0-06411
描述：

CVE(CAN) ID: CVE-2020-5129
SonicWall SMA100 是美国 SonicWall 公司的一款安全访问网关设备。
SonicWall SMA1000 12.1.0-06411 及之前版本的 HTTP Extraweb server 中存在安全漏洞。远程攻击者可利用该漏洞造成 HTTP 服务器崩溃，导致拒绝服务。
建议：

厂商补丁：
SonicWall
目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取

解决办法：
https://www.sonicwall.com/

➢ Apple macOS Catalina IOThunderboltFamily 组件资源管理错误漏洞

发布日期：2020-3-31
更新日期：2020-3-31
受影响系统：
Apple macOS Catalina <10.15.4
描述：

CVE(CAN) ID：CVE-2020-3851
Apple macOS Catalina 是美国苹果（Apple）公司的一套专为 Mac 计算机所开发的专用操作系统。
Apple macOS Catalina 10.15.4 之前版本中的 IOThunderboltFamily 组件存在资源管理错误漏洞。攻击者可利用该漏洞获取提升权限。
建议：

厂商补丁：
Apple
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://support.apple.com/en-us/HT211100

➢ IBM Spectrum Protect Plus 命令执行漏洞

发布日期：2020-04-1
更新日期：2020-04-1
受影响系统：
IBM Spectrum Protect Plus >=10.1.0，<=10.1.5
描述：

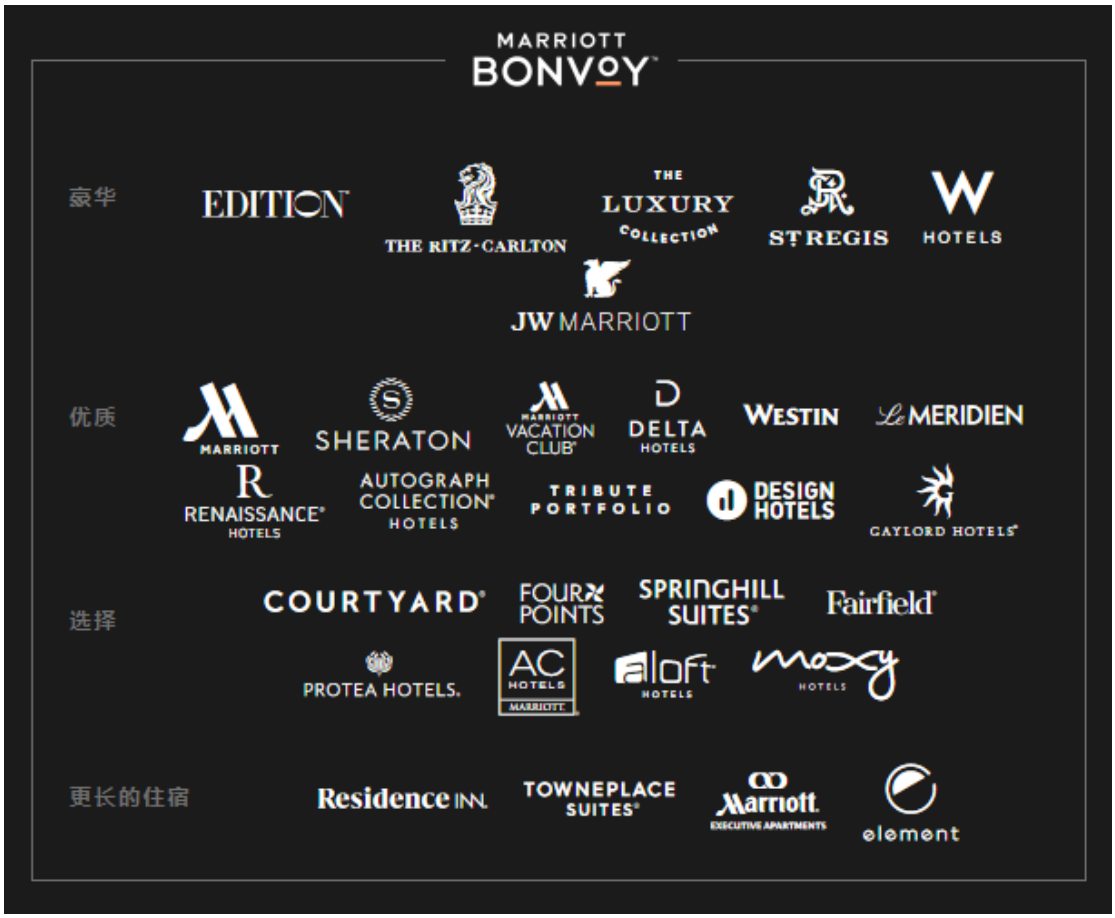
CVE(CAN) ID：CVE-2020-4241
BM Spectrum Protect Plus 是美国 IBM 公司的一套数据保护平台。该平台为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。
IBM Spectrum Protect Plus 10.1.0 版本至 10.1.5 版本中存在安全漏洞。远程攻击者可利用该漏洞通过发送特制的请求在系统上中执行任意命令。
建议：

厂商补丁：
IBM
厂商已发布了漏洞修复程序，请及时关注更新：
https://www.ibm.com/support/pages/node/6114130

六、本期网络安全事件

➢ 万豪披露又一起数据安全事件 520 万客户信息泄露

2020 年 4 月 1 日，万豪（Marriott）披露了旗下连锁酒店的又一起客户数据泄露事件。报道称事件发生于今年 1 月中旬，但直到 2 月下旬才被发现。调查发现有两名员工的登陆凭据有关，事件导致 520 万客户信息泄露。在堵上安全漏洞之后，万豪声称入侵者已被禁止访问。



在周二的公告中，万豪表示其发现了使用上述两个被盗的员工登陆凭据的“意外数量的来宾信息访问”。在封堵漏洞和禁用相关登陆凭据的同时，该公司声称还将增强监测能力。

确切的泄露细节，可能因不同的客户而异。万豪表示本次漏洞敞开了包括客户性别、生日、单位、会员账户积分、电话、邮件、邮寄地址、以及姓名等内容。庆幸的是，目前尚无证据表明某些重要客户的信息被泄露，包括驾照号码、银行卡信息、PIN 码或护照信息。不过随着时间的推移，后续可能有某些敏感信息被黑客曝光。

从 3 月 31 日起，万豪将通过电子邮件的方式，向可能受到本次安全漏洞影响的客户发

去通知。同时，酒店将为受影响的客户提供个人信息监控服务。需要指出的是，这并不是万豪连锁酒店首次曝出大规模的安全漏洞。比如 2019 年初的时候，其系统泄露了多达 500 万客户的未加密护照号码。

事件被发现与喜达屋的预订系统有关，影响自 2018 年 9 月 11 日前入住多达 3.83 亿的客户信息。不过除了万豪，希尔顿酒店也在 2015 年遭遇了两次不同的客户数据泄露事件，导致其被处以 70 万美元的罚款。（来源：cnBeta）

➢ Zoom 就隐私和安全问题道歉 并将冻结新功能以专注于修复各种问题

2020 年 4 月 2 日，Motherboard 网站在一份新报告中透露，Zoom 正在将成千上万个用户的私人信息泄露给陌生人，并使这些陌生人能够呼叫其他他们不认识的用户。上周，Motherboard 报告说，即使用户没有登录 Facebook 或没有 Facebook 帐户，Zoom 的 iOS 应用也正在向 Facebook 发送分析数据。不仅没有选择退出这种行为的方式，而且 Zoom 还没有提及数据将根据其隐私权政策发送给 Facebook。

在报告发布后不久，Zoom 就从其应用程序中删除了 Facebook SDK，但开始看起来 Facebook 只是 Zoom 隐私问题的冰山一角，近来涌现了许多问题。在 Motherboard 关于 Zoom 的最新报告中，揭示了该视频会议服务正在泄漏成千上万用户的电子邮件地址和照片，并让

陌生人试图对其进行呼叫。现在，Zoom 公司首席执行官 Eric S Yuan 向用户发表了冗长的声明，对不可预见的问题表示歉意，并承诺会进行改善。

Zoom 公司回应

Eric S Yuan 表示，Zoom 使用激增，从每天 1000 万用户跃升至 2 亿用户。Zoom 认识到没有达到社区的标准以及对个人隐私和安全的期望。为此，Zoom 深感抱歉。 现在，Zoom 有大量的用户在以各种意想不到的方式使用 Zoom 产品，这给他们带来了平台构想时无法预料的挑战。

Eric S Yuan 表示：“这些新的用例帮助我们发现了平台上无法预料的问题。记者和安全研究人员还帮助识别了先前存在的问题。我们感谢这些详细检查和疑问，其中包括有关服务的工作方式，我们的基础架构和容量，以及我们的隐私和安全政策。这些问题将使 Zoom 本身变得更加完善，为用户提供更好的服务。我们非常认真地对待这些详细检查和疑问，我们正在仔细研究每一个问题，并尽快解决它们。“

Zoom 已经采取了措施来回应对此提出的批评。该公司已更新了隐私政策，从其 iOS 应用中删除了 Facebook SDK，试图解决 Zoombombing 问题，修复了 UNC 链接的安全性问题，并阐明了其在端到端加密中的地位。

Eric S Yuan 解释了 Zoom 在接下来的几个月中还会做什么。在接下来的 90 天内，Zoom 致力于提供必要的资源，以更好地主动识别，解决和解决问题。Zoom 还致力于在整个过程中保持透明，Zoom 将尽一切努力保持您的信任，其中包括：立即冻结添加新功能，并立即转移所有工程资源以专注于最大的信任，安全和隐私问题。与第三方专家和代表用户进行全面审查，以了解并确保 Zoom 所有新消费者使用案例的安全性。准备透明度报告，其中详细说明了与数据，记录或内容请求有关的信息。增强当前的漏洞赏金计划。进行一系列白盒渗透测试，以进一步发现和解决问题。

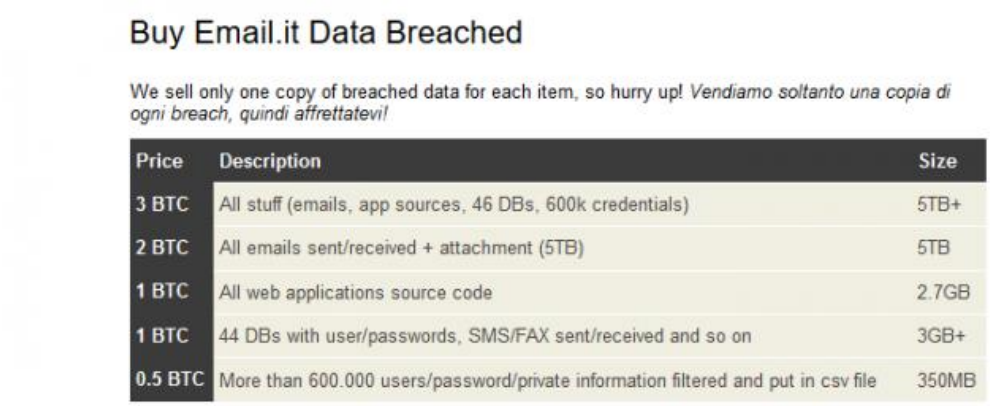
Eric S Yuan 表示，从下周开始，将在太平洋标准时间每周三上午 10 点举办每周一次的网络研讨会，向社区提供隐私和安全更新。（来源：互联网综合整理）

➢ 意大利电子邮件服务商被黑 60 万用户数据在暗网出售

2020 年 4 月 7 日，ZDNet 从一位读者提供的消息当中得知，目前有超过 60 万 Email.it 用户的数据正在暗网上被出售。这家意大利的电子邮件服务提供商周一向 ZDNet 表示：“不

幸的是，我们必须确认，我们遭遇了黑客的攻击。"

Email.it 黑客攻击在周日曝光，当时黑客们在 Twitter 上宣传了一个暗网网站，在该网站上出售公司的数据。黑客声称实际入侵发生在两年多前，即 2018 年 1 月，黑客入侵了 Email.it 数据中心，从服务器上拿走了任何可能的敏感数据，并选择给这家意大利的电子邮件服务提供商一个机会修补漏洞，同时要求们给黑客一点赏金，但是这家意大利的电子邮件服务提供商拒绝与黑客谈判，并继续欺骗它的用户。



Buy Email.it Data Breached

We sell only one copy of breached data for each item, so hurry up! *Vendiamo soltanto una copia di ogni breach, quindi affrettatevi!*

Price	Description	Size
3 BTC	All stuff (emails, app sources, 46 DBs, 600k credentials)	5TB+
2 BTC	All emails sent/received + attachment (5TB)	5TB
1 BTC	All web applications source code	2.7GB
1 BTC	44 DBs with user/passwords, SMS/FAX sent/received and so on	3GB+
0.5 BTC	More than 600.000 users/password/private information filtered and put in csv file	350MB

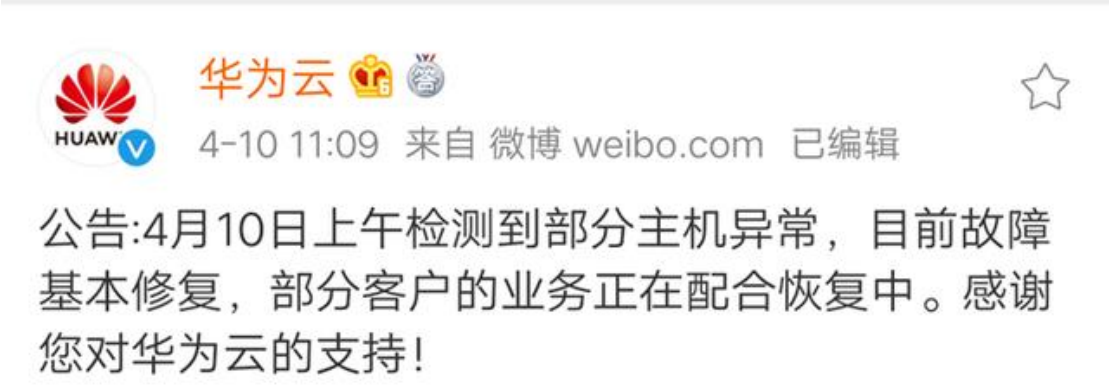
另外，黑客们在 2 月 1 日试图勒索 Email.it，当时他们要求对方支付赏金。Email.it 的一位发言人周一告诉 ZDNet，该公司拒绝支付，转而通知了意大利邮政警察局（CNAIPIC）。在勒索失败后，黑客们现在正在以 0.5 到 3 个比特币(3500 到 22000 美元)不等的要价出售该公司的数据。这些数据库包含了注册了免费 Email.it 电子邮件账户的用户信息。

黑客声称，这些数据库包含了 2007 年至 2020 年期间注册并使用该服务 60 多万用户的明文密码、安全问题、电子邮件内容和电子邮件附件。（来源：ZDNet）

➢ 华为云首次突发大规模“宕机”故障!云服务安全再引发行业关注

2020 年 4 月 10 日，上午 9 点起，“华为云崩了”“华为云挂了”等话题涌上热搜榜，在微博上引发网友热议。多位网友反映华为云官方网站登录不上去，管理后台无法访问。除了华为云登录，管理后台无法访问外，还出现了服务器暂时过载，连接错误等提示。有网友表示，此次故障对企业影响很大，公司电话已经被打爆，部门主管和运维在疯狂敲键盘。还有网友称，公司游戏全部宕机。

从网友众说纷纭中推测，此次的宕机事件或因北京机房出现故障导致，也有开发者称也许是存储服务出现问题造成的被迫关机。



事故发生后，华为方面进行了快速运维，截至中午 11 点 45 分，华为云在其微博上发布声明称基本业务已恢复，虽然已经得到官方修复公告的回应，但仍有不少用户表示“登录不上”。有网友表示，初步恢复到可登录的状态，用户信息数据库连不上，推测应该是虚拟化平台的问题。（来源：快科技）

➢ 300 元/小时接单 DDOS 攻击网游公司 大学生黑客被判刑

2020 年 4 月 10 日，为赚钱当起黑客，让游戏公司服务器瘫痪一个多小时。近日，经浙江省台州市黄岩区检察院提起公诉，该区法院采纳了检察机关提出的精准量刑建议，以破坏计算机信息系统罪一审判处骆某有期徒刑一年零十个月；而充当“网络打手”的凌某也因该罪被判处有期徒刑一年零三个月。据悉，这是浙江省台州市首例 DDOS 破坏网游公司计算机信息系统案。

2019 年 1 月，台州某智能科技公司陆续接到了不少游戏玩家投诉，反映在玩游戏时出现频频掉线等状况。该公司负责人随即向公安机关报案，从 2019 年 1 月 11 日开始，公司的网页服务器、游戏服务器等 20 余台服务器无故遭到不明 DDOS（分布式拒绝服务）攻击 256 次。这些攻击让用户无法登录，造成大量用户流失，仅一台服务器上受影响的注册用户人数就有近 2 万人，给公司造成了巨额损失。为了应对攻击，公司专门花费 5 万多元购买 DDOS 防护包，但效果并不显著。

公安机关随即立案侦查，通过调取该公司 IP 数据显示，2019 年 1 月 14 日，公司服务器系统崩溃达 1 小时 15 分。

经查，被告人骆某一直对网络知识有着浓厚兴趣，读大学一年级的时候，骆某就通过自学掌握了 IT 知识与技能，顺利考取全国信息技术应用培训教育工程师证书。因为头脑灵活，骆某在校期间还多次被评为“创业知青”。2018 年大学毕业后，骆某被安吉某科技公司聘任总经理一职，收入不菲。工作之余，骆某长期沉溺于网络，钻研黑客技术。其间，他发现一些论坛、QQ 群等平台会发布攻击网站、买卖攻击流量等信息，便觉得这是一条“生财之道”。骆某开始接受“客户”的雇用，从事网络攻击接单，并尝到了一些甜头。

2019 年 1 月，骆某以每小时 300 元的价格从“客户”处接单，要求攻击台州市某智能科技公司网站，把服务器 IP“打死”。骆某接单后，通过他原先加入的 QQ 群发单，将业务转包给同样懂得 DDOS 攻击技术的凌某（网名“黑猫”）等人从中赚取差价。

在接下该笔业务之前，无业在家的凌某与“小害虫”“天客”（网名，另案处理）等人合谋通过 DDOS 网络攻击服务器赚钱。三人建立了专门的 QQ 群，交流 DDOS 网络攻击技术。为承接攻击服务器业务，凌某等人合租了一台中控服务器，抓“肉鸡”（即黑客通过黑客扫描软件，将木马程序秘密植入防护能力较弱的计算机，进行“后门控制”，盗取最高管理权限）、通过域名把木马解析到服务器等。2019 年 1 月 14 日，凌某等人使用 DDOS 黑客攻击技术，轮流攻击上述公司服务器，致使该公司服务器不能正常运行。（来源：检察日报）

➢ 春雨医生、必胜客等 20 余款 APP 存涉嫌隐私不合规行为下架

2020 年 4 月 10 日，国家计算机病毒应急处理中心近期在“净网 2020”专项行动中对互联网监测发现，20 余款外卖、医疗和在线教育类移动应用存在涉嫌隐私不合规行为。

这些移动应用的违法违规行为主要有三大方面：

一是未向用户明示申请的全部隐私权限。具体 App 有《T11 生鲜超市》（版本 1.0.5）、《朴朴》（版本 2.7.5）、《美菜商城》（版本 2.17.1）、《蜂鸟跑腿》（版本 5.2.1）、《永辉生活》（版本 5.30.0.26）、《大润发优鲜》（版本 1.3.4）、《luckin coffee》（版本 3.5.0）、《每日优鲜》（版本 9.8.27）、《叮叮课堂》（版本 3.2.3）、《学霸君》（版本 5.7.2）、《人人讲》（版本 4.2.17）、《直播云》（版本 2.0.0.7）、《课后网》（版本 7.7.3.2.2）、《叮当快药》（版本 5.7.0）、《药师帮》（版本 4.31.0）、《健康云》（版本 5.1.3）、《1 药网》（版本 5.9.1）、《智慧好医院》（版本 2.1.3）、《春雨医生》（版本 8.8.8）、《洪恩识字》（版本 3.0.6）、《美岁直播》（版本 2.6.0）等。

二是未说明收集使用个人信息规则。具体 App 有《必胜客》（版本 5.6.5）、《平安好医生》（版本 7.2.0）。

三是未提供有效的更正、删除个人信息及注销用户账号功能。具体 App 有《好大夫》（版本 6.7.7）、《妙健康》（版本 5.1.10）。

针对上述情况，国家计算机病毒应急处理中心将对这些 App 进行通报下架处理，同时提醒广大手机用户：一是要谨慎下载使用，避免个人信息受到安全威胁；二是应打开手机中防病毒移动应用的“实时监控”功能，对手机操作进行主动防御，这样可以第一时间监控未知病毒的入侵活动。（来源：新华社）

信息安全意识产品服务

021-33663299