国盟信息安全通报

2022 年 4 月 30 日第 250 期

国盟信息安全通报

（第 250 期）

国际信息安全学习联盟

2022 年 04 月 30 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 369 个，其中高危漏洞 110 个、中危漏洞 219 个、低危漏洞 40 个。漏洞平均分值为 5.81。本周收录的漏洞中，涉及 0day 漏洞 192 个（占 52%），其中互联网上出现“AeroCMS 跨站脚本漏洞（CNVD-2022-30784）、CxuuCms 跨站脚本漏洞（CNVD-2022-31818）”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 9337 个，与上周（4626 个）环比增加 102%。

主要内容

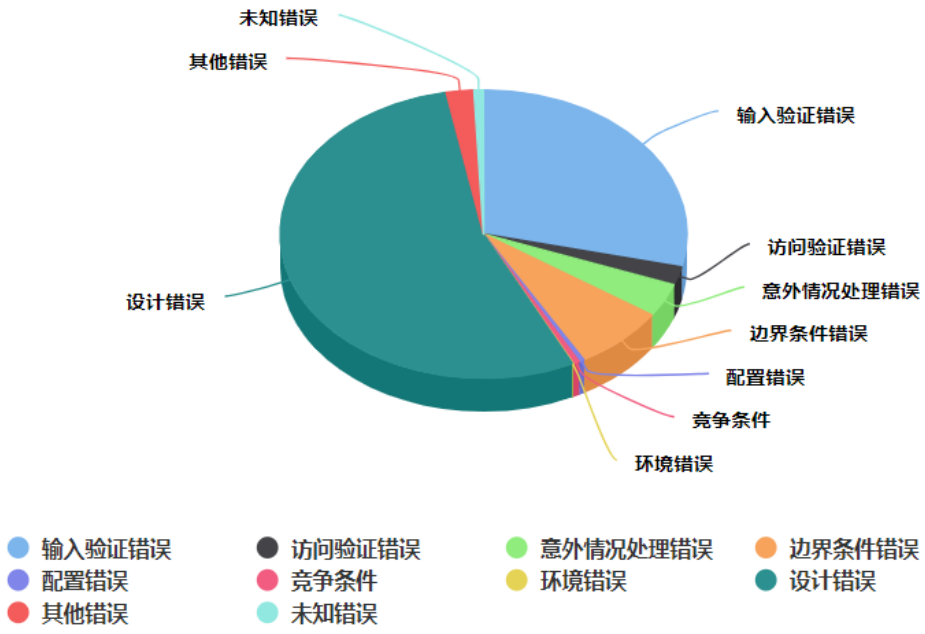
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

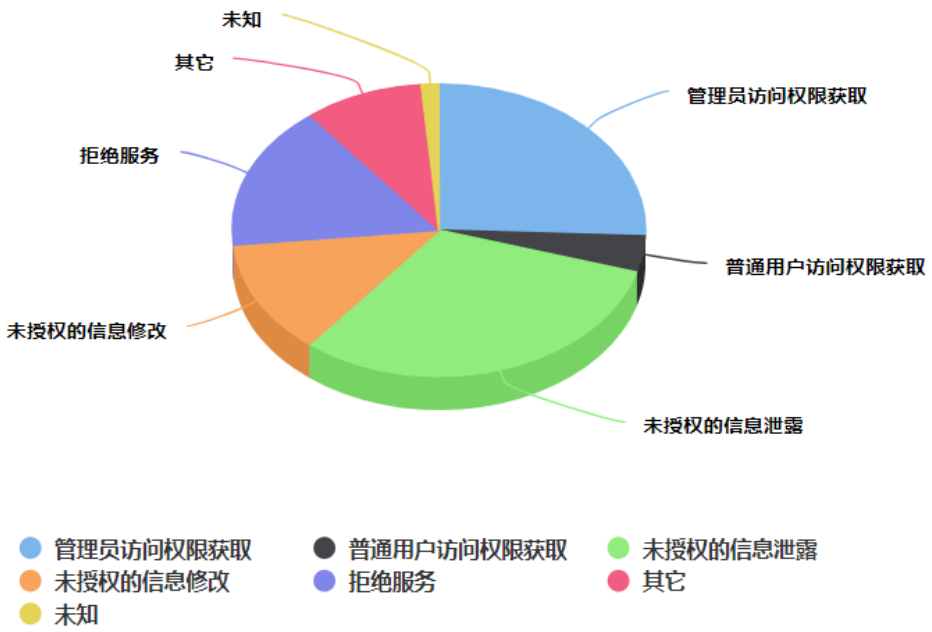
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 369 个，其中高危漏洞 110 个、中危漏洞 219 个、低危漏洞 40 个。漏洞平均分值为 5.81。本周收录的漏洞中，涉及 0day 漏洞 192 个（占 52%），其中互联网上出现“AeroCMS 跨站脚本漏洞（CNVD-2022-30784）、CxuuCms 跨站脚本漏洞（CNVD-2022-31818）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 9337 个，与上周（4626 个）环比增加 102%。

二、安全漏洞增长数量及种类分布情况

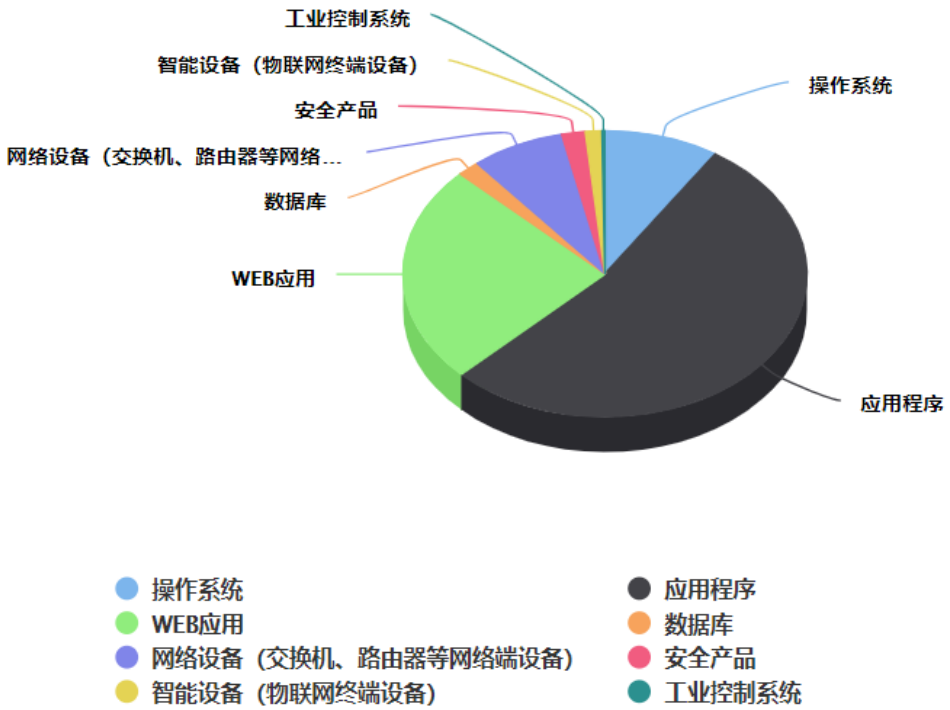
➢ 漏洞产生原因（2022 年 4 月 1 日—2022 年 4 月 30）



➢ 漏洞引发的威胁（2022 年 4 月 1 日—2022 年 4 月 30）



➢ 漏洞影响对象类型（2022 年 4 月 1 日—2022 年 4 月 30）



三、安全产业动态

➢ 习近平：保证国家安全是头等大事

党的十八大以来，习近平总书记创造性提出总体国家安全观，把我们党对国家安全的认识提升到了新的高度和境界，为破解我国国家安全面临的难题、推进新时代国家安全工作提供了基本遵循。以总体国家安全观为指引，我国国家安全得到全面加强，经受住了来自政治、经济、意识形态、自然界等各方面的风险挑战考验，为党和国家兴旺发达、长治久安提供了有力保证。2022 年 4 月 15 日是第七个“全民国家安全教育日”，今年活动的主题是“树牢总体国家安全观，感悟新时代国家安全成就，为迎接党的二十大胜利召开营造良好氛围”。我们摘录了习近平总书记关于国家安全的重要论述，一起学习，共同增强国家安全意识。

保证国家安全是头等大事

国家安全是国家生存发展的基本前提，维护国家安全是全国各族人民根本利益所在。当今世界，兵戎相见时有发生，冷战思维和强权政治阴魂不散，恐怖主义、难民危机、重大传染性疾病、气候变化等非传统安全威胁持续蔓延。种种景象深刻启示我们：没有国家安全的基础，任何美好蓝图都是空中楼阁。习近平总书记高度重视国家安全问题，多次强调要增强忧患意识，做到居安思危，把安全发展贯穿国家发展各领域全过程。

【总书记说】

国家安全和社会稳定是改革发展的前提。只有国家安全和社会稳定，改革发展才能不断

推进。——2013 年 11 月 9 日关于《中共中央关于全面深化改革若干重大问题的决定》的说明

增强忧患意识，做到居安思危，是我们治党治国必须始终坚持的一个重大原则。我们党要巩固执政地位，要团结带领人民坚持和发展中国特色社会主义，保证国家安全是头等大事。——2014 年 4 月 15 日在中央国家安全委员会第一次会议上的讲话

推动创新发展、协调发展、绿色发展、开放发展、共享发展，前提都是国家安全、社会稳定。没有安全和稳定，一切都无从谈起。——2016 年 1 月 18 日在省部级主要领导干部学习贯彻党的十八届五中全会精神专题研讨班上的讲话

国泰民安是人民群众最基本、最普遍的愿望。实现中华民族伟大复兴的中国梦，保证人民安居乐业，国家安全是头等大事。——2016 年在 4 月 15 日首个全民国家安全教育日到来之际作出的指示

国家安全是安邦定国的重要基石，维护国家安全是全国各族人民根本利益所在。——2017 年 10 月 18 日在中国共产党第十九次全国代表大会上的报告

前进的道路不可能一帆风顺，越是前景光明，越是要增强忧患意识，做到居安思危，全面认识和有力应对一些重大风险挑战。要聚焦重点，抓纲带目，着力防范各类风险挑战内外联动、累积叠加，不断提高国家安全能力。——2018 年 4 月 17 日在十九届中央国家安全委员会第一次会议上的讲话

我们越来越深刻地认识到，安全是发展的前提，发展是安全的保障。当前和今后一个时期是我国各类矛盾和风险易发期，各种可以预见和难以预见的风险因素明显增多。我们必须坚持统筹发展和安全，增强机遇意识和风险意识，树立底线思维，把困难估计得更充分一些，把风险思考得更深入一些，注重堵漏洞、强弱项，下好先手棋、打好主动仗，有效防范化解各类风险挑战，确保社会主义现代化事业顺利推进。——2020 年 11 月 3 日关于《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》的说明

国家安全工作是党治国理政一项十分重要的工作，也是保障国泰民安一项十分重要的工作。——2020 年 12 月 11 日在十九届中央政治局第二十六次集体学习时的讲话

“不困在于早虑，不穷在于早豫。”随着我国社会主要矛盾变化和国际力量对比深刻调整，我国发展面临的内外部风险空前上升，必须增强忧患意识、坚持底线思维，随时准备应对更加复杂困难的局面。——2021 年 1 月 11 日在省部级主要领导干部学习贯彻党的十九届五中全会精神专题研讨班上的讲话

准确把握国家安全形势变化新特点新趋势

习近平总书记指出，随着我国社会主要矛盾变化和国际力量对比深刻调整，我国发展面临的内外部风险空前上升；国家安全内涵和外延比历史上任何时候都要丰富，时空领域比历史上任何时候都要宽广，内外因素比历史上任何时候都要复杂。总书记的重要论述指明了新时代我国国家安全所处的历史方位，是我们在新征程上准确识变、科学应变、主动求变的基本坐标和依据。

【总书记说】

当前我国国家安全内涵和外延比历史上任何时候都要丰富，时空领域比历史上任何时候都要宽广，内外因素比历史上任何时候都要复杂，必须坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，走出一条中国特色国家安全道路。——2014 年 4 月 15 日在中央国家安全委员会第一次会议上的讲话

改革开放以来，我们党始终高度重视正确处理改革发展稳定关系，始终把维护国家安全和社会安定作为党和国家的一项基础性工作。我们保持了我国社会大局稳定，为改革开放和社会主义现代化建设营造了良好环境。“安而不忘危，存而不忘亡，治而不忘乱。”同时，必须清醒地看到，新形势下我国国家安全和社会安定面临的威胁和挑战增多，特别是各种威胁和挑战联动效应明显。我们必须保持清醒头脑、强化底线思维，有效防范、管理、处理国家安全风险，有力应对、处置、化解社会安定挑战。——2014 年 4 月 25 日在十八届中央政治局第十四次集体学习时的讲话

今后 5 年，可能是我国发展面临的各方面风险不断积累甚至集中显露的时期。我们面临的重大风险，既包括国内的经济、政治、意识形态、社会风险以及来自自然界的风险，也包括国际经济、政治、军事风险等。如果发生重大风险又扛不住，国家安全就可能面临重大威胁，全面建成小康社会进程就可能被迫中断。我们必须把防风险摆在突出位置，“图之于未萌，虑之于未有”，力争不出现重大风险或在出现重大风险时扛得住、过得去。——2015 年 10 月 29 日在十八届五中全会第二次全体会议上的讲话

认清国家安全形势，维护国家安全，要立足国际秩序大变局来把握规律，立足防范风险的大前提来统筹，立足我国发展重要战略机遇期大背景来谋划。——2017 年 2 月 17 日在国家安全工作座谈会上的讲话

“备豫不虞，为国常道”。当前，我国正处于一个大有可为的历史机遇期，发展形势总的是好的，但前进道路不可能一帆风顺，越是取得成绩的时候，越是要有如履薄冰的谨慎，越是要有居安思危的忧患，绝不能犯战略性、颠覆性错误。——2018 年 1 月 5 日在新进中

央委员会的委员、候补委员和省部级主要领导干部学习贯彻习近平新时代中国特色社会主义思想和党的十九大精神研讨班上的讲话

新形势下，我国面临复杂多变的发展和安全环境，各种可以预见和难以预见的风险因素明显增多，如果得不到及时有效控制也有可能演变为政治风险。全党同志特别是各级领导干部必须增强风险意识，提高防范政治风险能力。——2018 年 6 月 29 日在十九届中央政治局第六次集体学习时的讲话

当前，世界大变局加速深刻演变，全球动荡源和风险点增多，我国外部环境复杂严峻。我们要统筹国内国际两个大局、发展安全两件大事，既聚焦重点、又统揽全局，有效防范各类风险连锁联动。——2019 年 1 月 21 日在省部级主要领导干部坚持底线思维着力防范化解重大风险专题研讨班上的讲话

新的征程上，我们必须增强忧患意识、始终居安思危，贯彻总体国家安全观，统筹发展和安全，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，深刻认识我国社会主要矛盾变化带来的新特征新要求，深刻认识错综复杂的国际环境带来的新矛盾新挑战，敢于斗争，善于斗争，逢山开道、遇水架桥，勇于战胜一切风险挑战！——2021 年 7 月 1 日在庆祝中国共产党成立 100 周年大会上的讲话

坚持总体国家安全观，走中国特色国家安全道路

坚持总体国家安全观，必须坚持国家利益至上，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、科技、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全，构建国家安全体系，走出一条中国特色国家安全道路。总体国家安全观关键在“总体”，突出的是“大安全”理念，强调的是做好国家安全工作的系统思维和方法。

【总书记说】

贯彻落实总体国家安全观，必须既重视外部安全，又重视内部安全，对内求发展、求变革、求稳定、建设平安中国，对外求和平、求合作、求共赢、建设和谐世界；既重视国土安全，又重视国民安全，坚持以民为本、以人为本，坚持国家安全一切为了人民、一切依靠人民，真正夯实国家安全的群众基础；既重视传统安全，又重视非传统安全，构建集政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、信息安全、生态安全、资源安全、核安全等于一体的国家安全体系；既重视发展问题，又重视安全问题，发展是安全的基础，安全是发展的条件，富国才能强兵，强兵才能卫国；既重视自身安全，又重视共同安全，打造命运共同体，推动各方朝着互利互惠、共同安全的目标相向而行。——2014 年 4 月 15 日在中央国家安全委员会第一次会议上的讲话

要坚持国家安全一切为了人民、一切依靠人民，动员全党全社会共同努力，汇聚起维护国家安全的强大力量，夯实国家安全的社会基础，防范化解各类安全风险，不断提高人民群众的安全感、幸福感。——2016 年在 4 月 15 日首个全民国家安全教育日到来之际作出的指示

统筹发展和安全，增强忧患意识，做到居安思危，是我们党治国理政的一个重大原则。必须坚持国家利益至上，以人民安全为宗旨，以政治安全为根本，统筹外部安全和内部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全，完善国家安全制度体系，加强国家安全能力建设，坚决维护国家主权、安全、发展利益。——2017 年 10 月 18 日在中国共产党第十九次全国代表大会上的报告

全面贯彻落实总体国家安全观，必须坚持统筹发展和安全两件大事，既要善于运用发展成果夯实国家安全的实力基础，又要善于塑造有利于经济社会发展的安全环境；坚持人民安全、政治安全、国家利益至上的有机统一，人民安全是国家安全的宗旨，政治安全是国家安全的根本，国家利益至上是国家安全的准则，实现人民安居乐业、党的长期执政、国家长治久安；坚持立足于防，又有效处置风险；坚持维护和塑造国家安全，塑造是更高层次更具前瞻性的维护，要发挥负责任大国作用，同世界各国一道，推动构建人类命运共同体；坚持科学统筹，始终把国家安全置于中国特色社会主义事业全局中来把握，充分调动各方面积极性，形成维护国家安全合力。——2018 年 4 月 17 日在十九届中央国家安全委员会第一次会议上的讲话

做好新时代国家安全工作，要坚持总体国家安全观，抓住和用好我国发展的重要战略机遇期，把国家安全贯穿到党和国家工作各方面全过程，同经济社会发展一起谋划、一起部署，坚持系统思维，构建大安全格局，促进国际安全和世界和平，为建设社会主义现代化国家提供坚强保障。——2020 年 12 月 11 日在十九届中央政治局第二十六次集体学习时的讲话

树立共同、综合、合作、可持续的全球安全观

在经济全球化时代，安全问题早已超越国界，各国可谓安危与共、唇齿相依，没有哪个国家能够置身事外而独善其身，也没有哪个国家可以包打天下来实现所谓的绝对安全。习近平总书记倡导共同、综合、合作、可持续的全球安全观，为解开世界安全困局、实现持久和平与共同安全指明了方向。

【总书记说】

国际社会应该倡导综合安全、共同安全、合作安全的理念，使我们的地球村成为共谋发展的大舞台，而不是相互角力的竞技场，更不能为一己之私把一个地区乃至世界搞乱。——

2013 年 4 月 7 日在博鳌亚洲论坛 2013 年年会上的讲话

“明者因时而变，知者随事而制。”形势在发展，时代在进步。要跟上时代前进步伐，就不能身体已进入 21 世纪，而脑袋还停留在冷战思维、零和博弈的旧时代。我们认为，应该积极倡导共同、综合、合作、可持续的亚洲安全观，创新安全理念，搭建地区安全和合作新架构，努力走出一条共建、共享、共赢的亚洲安全之路。——2014 年 5 月 21 日在亚洲相互协作与信任措施会议第四次峰会上的讲话

在经济全球化时代，各国安全相互关联、彼此影响。没有一个国家能凭一己之力谋求自身绝对安全，也没有一个国家可以从别国的动荡中收获稳定。弱肉强食是丛林法则，不是国与国相处之道。穷兵黩武是霸道做法，只能搬起石头砸自己的脚。——2015 年 9 月 28 日在第七十届联合国大会一般性辩论时的讲话

人类生存在同一个地球上，一国安全不能建立在别国不安全之上，别国面临的威胁也可能成为本国的挑战。面对日益复杂化、综合化的安全威胁，单打独斗不行，迷信武力更不行。我们应该坚持共同、综合、合作、可持续的新安全观，营造公平正义、共建共享的安全格局，共同消除引发战争的根源，共同解救被枪炮驱赶的民众，共同保护被战火烧灼的妇女儿童，让和平的阳光普照大地，让人人享有安宁祥和。——2017 年 12 月 1 日在中国共产党与世界政党高层对话会上的讲话

我们要践行共同、综合、合作、可持续的安全观，摒弃冷战思维、集团对抗，反对以牺牲别国安全换取自身绝对安全的做法，实现普遍安全。——2018 年 6 月 10 日在上海合作组织成员国理事会第十八次会议上的讲话

我们要秉持共同、综合、合作、可持续的新安全观，摒弃冷战思维、零和博弈的旧思维，摒弃弱肉强食的丛林法则，以合作谋和平、以合作促安全，坚持以和平方式解决争端，反对动辄使用武力或以武力相威胁，反对为一己之私挑起事端、激化矛盾，反对以邻为壑、损人利己，各国一起走和平发展道路，实现世界长久和平。——2019 年 3 月 26 日在中法全球治理论坛闭幕式上的讲话

要倡导共同、综合、合作、可持续的安全观，通过协商和谈判化解分歧，反对干涉内政，反对单边制裁和“长臂管辖”，共同营造和平稳定的发展环境。——2020 年 11 月 17 日在金砖国家领导人第十二次会晤上的讲话

我们向来从事情本身的是非曲直出发，独立自主作出判断，倡导维护国际法和公认的国际关系基本准则，坚持按照联合国宪章办事，主张共同、综合、合作、可持续的安全观。——2022 年 3 月 18 日同美国总统拜登视频通话时的讲话 （来源：求是网）

➢ 顺应信息革命时代潮流 奋力推进网络强国建设

习近平总书记指出：“从社会发展史看，人类经历了农业革命、工业革命，正在经历信息革命。”“信息化为中华民族带来了千载难逢的机遇。”党的十八大以来，以习近平同志为核心的党中央着眼全局、把握大势，主动顺应信息革命发展潮流，高度重视、全面布局、统筹推进网络安全和信息化工作，推动网信事业取得历史性成就、发生历史性变革。习近平总书记举旗定向、掌舵领航，提出一系列具有开创性意义的新思想新观点新论断，系统回答了为什么要建设网络强国、怎样建设网络强国的重大理论和实践问题，形成了内涵丰富、科学系统的习近平总书记关于网络强国的重要思想。在习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想指引下，网络安全和信息化各项工作扎实有力推进，我国正从网络大国向网络强国阔步迈进。

坚持政治统领，切实加强党对网信工作的全面领导

党的十八大以来，以习近平同志为核心的党中央站在巩固党的长期执政地位的政治高度，强调“过不了互联网这一关就过不了长期执政这一关”，把党管互联网作为重要政治原则，科学把握互联网管理的全局性、系统性、协同性特点，改革和完善互联网管理领导体制机制，着力加强党中央对网信工作的集中统一领导。完善领导体制，成立中央网络安全和信息化领导小组(后改为委员会)，习近平总书记亲自领导、亲自指挥、亲自部署，强化网信领域顶层设计、总体布局、统筹协调、整体推进和督促落实。中央、省、市三级网信工作体系基本建立，县级网信机构建设扎实推进。加强顶层设计，组织编辑出版和深入学习贯彻《习近平关

于网络强国论述摘编》，制定出台《关于加强网络安全和信息化工作的意见》《关于加快建立网络综合治理体系的意见》《国家网络空间安全战略》《国家信息化发展战略纲要》和“十四五”相关规划等文件，完善各领域、多层级协调机制，统筹推进网信领域重要任务、重大项目、重点工程。压实政治责任，制定实施《党委(党组)网络意识形态工作责任制实施细则》《党委(党组)网络安全工作责任制实施办法》，把党管互联网落到实处;深化全面从严治党，加强网信系统党的建设和干部人才队伍建设，营造风清气正的政治生态，打造忠诚干净担当的网信铁军。

坚持举旗铸魂，同心唱响网络空间团结奋进时代强音

面对互联网对意识形态工作带来的新课题新挑战，以习近平同志为核心的党中央从进行具有许多新的历史特点的伟大斗争出发，强调“党高度重视互联网这个意识形态斗争的主阵地、主战场、最前沿”，“要把网上舆论工作作为宣传思想工作的重中之重来抓”。全国网信系统坚持正能量是总要求、管得住是硬道理、用得好是真本事，牢牢把握网络意识形态工作主导权和主动权，让党的声音始终成为网络空间最强音。强化思想引领，坚持把习近平新时代中国特色社会主义思想网上宣传作为头等大事，紧紧围绕习近平总书记重要会议、重要讲话、重要活动，建强网上理论阵地，创新语态表达和互动引导，精心打造“学习进行时”“理上网来”等专题专栏，积极做好“奋斗百年路 启航新征程”等重大主题宣传，全方位、立体化展现习近平总书记大国大党领袖风范。壮大主流舆论，守正创新做好网上重大主题宣传和重大议题设置，涵盖党史学习教育、全面深化改革、脱贫攻坚、疫情防控等重点领域，每年百余项主题宣传统筹推进、亮点纷呈;创新网上正面宣传，举办中国正能量“五个一百”网络精品征集评选展播活动，建设“正能量稿池”，大力营造强信心、聚民心、暖人心、筑同心的浓厚氛围;加强和改进网络国际传播工作，努力塑造可信、可爱、可敬的中国形象。坚守网上阵地，强化风险意识和底线思维，建立健全网上舆情引导工作机制、网上风险防范机制，稳妥调控各类突发敏感舆情;敢于亮剑、敢于斗争，有力批驳历史虚无主义等错误思想观点，坚决清理造谣污蔑言论、暴恐音视频等各类有害信息，加强网络举报处置，打造中国互联网联合辟谣平台，强化新技术新应用安全风险评估，有力维护网络意识形态安全和政治安全。

坚持综合治理，努力营造天朗气清的良好网络生态

加快建立网络综合治理体系，是提升治网管网能力、营造清朗网络空间的治本之策。习近平总书记指出：“必须提高网络综合治理能力，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局。”全国网信系统坚持系统性谋划、综合性治理、体系化推进，广泛凝聚网络综合治理的工作合

力。深化网络生态治理，持续开展“清朗”系列专项行动，对“饭圈”乱象、色情低俗、血腥暴力、网络水军、流量造假、网络“黑公关”等突出问题出重拳、亮利剑，集中清理负面有害信息、违法违规账号与移动应用程序，赢得了广大网民的积极支持和充分肯定。压实平台主体责任，认真落实“两个所有”要求，推动将所有从事新闻信息服务、具有媒体属性和舆论动员功能的传播平台都纳入管理范围，所有新闻信息服务和相关业务从业人员都实行准入管理;督促网站平台完善社区规则、规范内部管理、提升内容质量，构建全流程、全链条监管体系，网络传播秩序更加规范。推进网络文明建设，以中办、国办名义印发《关于加强网络文明建设的意见》，成功创办首届中国网络文明大会;大力培育和践行社会主义核心价值观，实施争做中国好网民工程、网络公益工程、网络文明伙伴行动，推动网络诚信理念更加深入人心;加强互联网企业党建工作，党的组织覆盖率和工作覆盖率显著提升;走好网上群众路线，引导亿万网民共建网上美好精神家园。

坚持筑牢屏障，有力维护国家网络安全、数据安全和个人信息安全

习近平总书记指出：“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”全国网信系统坚持发展和安全同步推进，加强网络安全保障体系和能力建设，推动全社会网络安全意识和防护能力明显增强。强化关键信息基础设施安全保护，针对水利、电力、油气、交通、通信、金融等领域重要信息基础设施，着力提升防护水平;实施《网络安全审查办法》《云计算服务安全评估办法》，组织开展对关键信息基础设施运营者采购网络产品和服务活动的网络安全审查，组织对面向党政机关和关键信息基础设施服务的云平台开展安全评估，有效防范安全风险。强化网络安全工作基础，健全国家

网络安全应急体系，实施《国家网络安全事件应急预案》，全面提升网络安全态势感知、事件分析、追踪溯源、应急处置能力;连续 8 年举办国家网络安全宣传周，增设网络空间安全一级学科，建设国家网络安全人才与创新基地，推动形成多方参与、优势互补、融合发展的网络安全良性生态。强化数据安全管理和个人信息保护，出台《汽车数据安全管理若干规定(试行)》，研究起草网络数据安全管理条例、数据出境安全评估办法，规范数据处理活动;深入开展 App 违法违规收集使用个人信息专项治理，严厉打击非法买卖个人信息、侵犯公民隐私、电信网络诈骗等违法犯罪活动，有力维护了人民群众的合法权益。

坚持自立自强，坚决打好信息领域核心技术攻坚战

加快核心技术突破，是抢占信息时代发展主动权、竞争主导权的关键所在。习近平总书记指出：“互联网核心技术是我们最大的‘命门’，核心技术受制于人是我们最大的隐患。”“核心技术是国之重器，最关键最核心的技术要立足自主创新、自立自强。”全国网信系统紧紧牵住核心技术自主创新“牛鼻子”，着力推动核心技术发展从跟跑到并跑、领跑的转变。加强前沿技术攻关，瞄准国家重大战略需求，集中资源力量加大攻关力度，我国软件和集成电路技术加快发展，国产操作系统应用深入推进，大数据、云计算、人工智能、区块链等研究取得积极进展，量子通信、量子计算等领域实现原创性突破，世界超级计算机 500 强中上榜总数多年蝉联第一，光存储、基础软件、核心元器件等关键共性技术取得重要成果，部分领域形成全球竞争优势。培育良好产业生态，充分发挥我国社会主义制度优势、新型举国体制优势、超大规模市场优势，加快建立自主产业生态体系，持续打通创新链、产品链、价值链，强化上下游衔接互动，技术创新与实际应用形成正向循环。强化政策支撑保障，打好科技、金融、财政、税收、产业等方面政策“组合拳”，积极构建以企业为主体、市场为导向、产学研深度融合的技术创新体系，数字科技专利申请数量保持领先，“揭榜挂帅”机制布局实施，基本形成政策协同、上下联动、资源整合的工作格局。

坚持驱动引领，着力以信息化为经济社会高质量发展赋能增效

习近平总书记指出：“网信事业代表着新的生产力和新的发展方向，应该在践行新发展理念上先行一步。”“以信息化培育新动能，用新动能推动新发展。”全国网信系统坚持把握新发展阶段、贯彻新发展理念、构建新发展格局，加快建设网络强国、数字中国、智慧社会，以信息化推进国家治理体系和治理能力现代化，为经济社会高质量发展注入强劲动能。加快完善基础设施，统筹推进 5G、IPv6、数据中心、卫星互联网、物联网等建设发展，建成全球规模最大的 4G、5G 和光纤宽带网络，IPv6 地址数量跃居全球第一、活跃用户数达 6.35 亿，北斗导航系统已在 20 多个国家开通高精度服务、总用户数超过 20 亿。大力发展数字经济，

我国数字经济规模连续多年位居全球第二，其中电子商务交易额、移动支付交易规模位居全球第一，一批网信企业跻身世界前列;推动实施“互联网+”行动计划、国家大数据战略，促进数字技术和实体经济深度融合，推动数字化绿色化协同转型发展，数字产业化和产业数字化成效显著;优化数字经济发展环境，强化互联网领域反垄断和防止资本无序扩张，促进互联网企业健康有序发展。全面建设数字社会，坚持以人民为中心的发展思想，推进“互联网+政务服务”，全国一体化政务服务平台实名用户超 9 亿，“一网通办”“最多跑一次”广泛实践，“数字抗疫”取得积极成效;分级分类推进新型智慧城市建设，深入开展人工智能社会实验，建设国家智能社会治理实验基地;以数字化促进共同富裕，接续推进网络扶贫和数字乡村建设，实施全民数字素养与技能提升行动，让亿万人民共享互联网发展成果;举办数字中国建设峰会，广泛凝聚共建数字中国整体合力。2012 年 12 月至 2021 年 12 月，我国网民规模由 5.64 亿增长到 10.32 亿，互联网普及率从 42.1%提升到 73%，形成了全球最大、生机勃勃的数字社会。

坚持固本强基，加快推进网络空间法治化进程

习近平总书记高度重视法治在网络强国建设中的基础性作用，强调“网络空间不是‘法外之地’。”“要坚持依法治网、依法办网、依法上网，让互联网在法治轨道上健康运行。”全国网信系统坚持把依法治网摆在突出位置，推动网络法治工作取得积极进展和重要成果。加快网络立法，出台《中华人民共和国网络安全法》《中华人民共和国电子商务法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》等法律法规，《互联网新闻信息服务管理规定》《网络信息内容生态治理规定》《儿童个人信息网络保护规定》《区块链信息服务管理规定》等部门规章，以及《网络音视频信息服务管理规定》《互联网用户公众账号信息服务管理规定》等规范性文件，完成了网络法律体系的基本构建。强化网络执法，发挥执法利剑震慑作用，通过执法约谈、责令整改、下架、停更、罚款、通报等手段对违法违规问题予以坚决惩处;加强网络执法统筹指导，优化网络执法工作机制，着力提升网络执法、督查、队伍建设协同性整体性。深化网络普法，加强网络普法形式、内容、手段等创新，深入实施网信系统“七五”“八五”普法规划，持续推动全国网络普法进机关、进企业、进学校、进社区、进农村、进军营、进网络，着力营造全社会尊法学法守法用法的良好氛围。

坚持开放共享，积极推动构建网络空间命运共同体

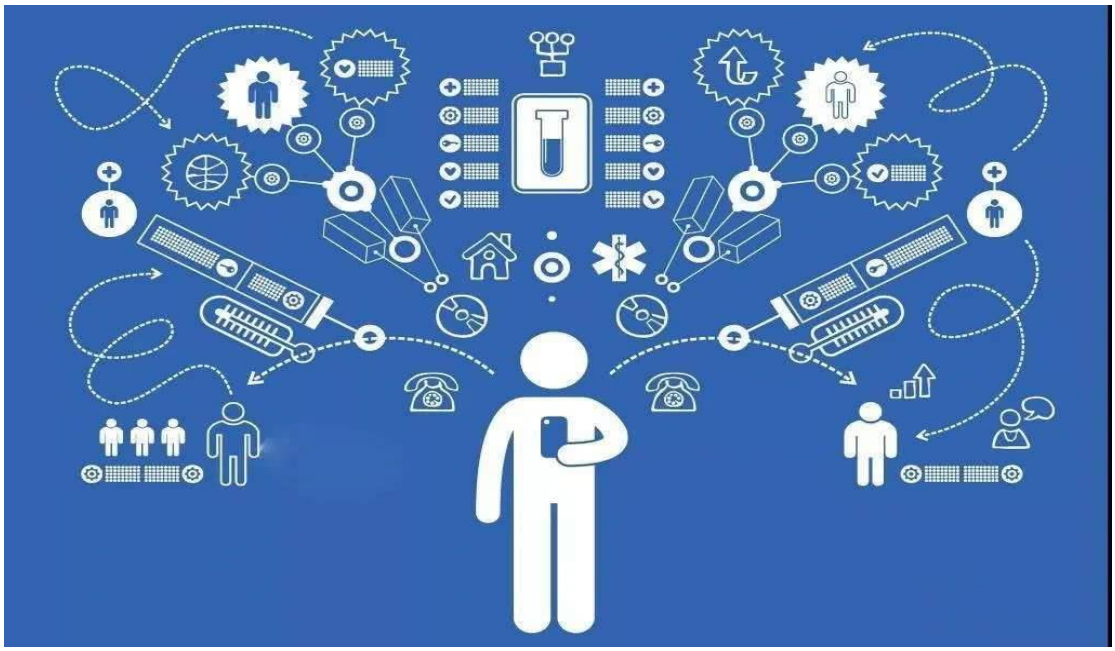
习近平总书记深刻洞察全球互联网发展大势，创造性提出推进全球互联网治理体系变革“四项原则”和构建网络空间命运共同体“五点主张”，为全球互联网发展治理贡献了中国

智慧和中国方案。全国网信系统以“四项原则”“五点主张”为指引，着眼高水平对外开放，推动网络空间国际交流合作向纵深发展。积极搭建合作平台，连续 8 年举办世界互联网大会，先后邀请多国政要和政府官员、国际组织负责人、国内外知名互联网企业代表等参会交流、共话发展，形成了携手构建网络空间命运共同体概念文件和行动倡议、《网络主权：理论与实践》等一系列重要成果，有力搭建中国与世界互联互通的国际平台和国际互联网共享共治的中国平台。深入开展国际交流，主动参与数字领域国际规则制定，深度参与联合国互联网治理论坛等网络空间国际治理多边活动，发布由我国牵头制定的《二十国集团数字经济发展与合作倡议》，有力促进全球互联网治理体系改革完善。持续扩大务实合作，打造多层次全球数字合作伙伴关系，运筹好大国网络关系，深化同新兴市场国家、发展中国家网信合作交流，举办 APEC 数字减贫研讨会、中国—东盟信息港论坛、中非互联网发展与合作论坛、中俄网络媒体论坛，加强 21 世纪数字丝绸之路建设和 5G 等信息通信技术合作，推动构建和平、安全、开放、合作、有序的网络空间。

万山磅礴看主峰，大潮奔涌好扬帆。面向新时代新征程，我们将更加紧密团结在以习近平同志为核心的党中央周围，以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导，深刻认识“两个确立”的决定性意义，增强“四个意识”、坚定“四个自信”、做到“两个维护”，踔厉奋发、勇毅前行，在全面建设社会主义现代化国家新征程上奋力谱写网络强国建设新篇章，以优异成绩迎接党的二十大胜利召开。（来源:《学习时报》2022 年 4 月 20 日第 1 版　作者：中央宣传部副部长，中央网信办主任、国家网信办主任庄荣文）

➢ 筑牢网络安全防线，需要从哪些方面努力？

2022 年 4 月 29 日是第九个“首都网络安全日”，这个纪念日旨在展示网络安全建设成果，倡导社会各界承担网络安全责任，投身网络安全建设，维护网络生态环境。如今面对钓鱼邮件、不明二维码、公共 Wi-Fi 陷阱等，我们已经有了一定的辨别能力，但随着新的硬件设备、网络服务形态、技术使用场景不断多样，网络安全的整体形势依然较为严峻。这个过程当中，我们当然要关注自己的网络使用习惯，与此同时，我们国家标准的不断完善和补充，也正在为网络安全提供助力和规范。当我们关注网络安全时我们到底在关注什么？在网络安全方面，“国家标准”是个什么样的存在？筑牢网络安全防线，我们还可以从哪些方面继续努力？



当我们关注网络安全时我们在关注什么？

中国科学院大学计算机科学与技术学院数据保护研究中心教授、全国信安标委身份鉴别与授权工作组组长荆继武表示：“网络攻防、网络治理、网络资产的维护和增值，以及网络经济发展都属于网络安全要去研究和推动的问题。”

一方面，网络安全必须强调网络治理，要将法律精神置于网络环境，人们在网络上各司其职，才能降低网络防御的成本。另一方面，网络财富管理也是网络安全的重要组成部分。当网络经济发展到一定程度时，网络财富和个人资产变得更为重要，因此，必须要加大力度保护好用户隐私和数据安全。

网络安全方面的“国家标准”是如何制定的？

全国信息安全标准化技术委员会是专注于整个网络专业化安全标准制定的机构，网络安全方面的“国家标准”就由该部门制定。

标准从起草到最终落地需要经历多个环节，在标准的申请阶段，由整个工作组根据网络社会的发展和需要，提出一个大家关注的问题。随后进入对这一问题的研究阶段，一般为期一年。如果遇到着急情况，且工作组成员达成共识，可省略研究阶段直接进入研制阶段。荆继武表示，按照国家标准化技术委员会的相关规定，标准的研制需要先讨论立项，随后面向全社会征求意见，接着再报批送审等，最后标准才能落地。标准有强制性和推荐性之分。国家对于强制性标准要求严格，但网络安全的标准大部分是推荐性的，目的在于信息技术不断发展变化中需要鼓励创新。

筑牢网络安全防线，需要从哪些方面努力？

用户需要了解网络安全相关知识，尽量选择符合国家相关标准或是通过了相关机构检测认证的软件。因为在发展初期，相关标准还未成熟，需要靠企业自己执行，所以有信用的大企业的软件更值得选择。但网络没有绝对的安全，只要使用互联网就可能存在风险。因此，学术界应该不断研发简单易用，同时隐藏在系统底层，能够帮助用户解决安全问题的技术。荆继武称：“尽量把对安全的影响降到最低，同时又带给大家便利，这是我们一直以来的研究方向。”而产业界则要按照标准行事，要参与标准的制定，推动标准的落地，大家都按同一个标准去做，风险才能下降。（来源：新华网）

➢ 贯彻总体国家安全观 切实筑牢数据安全屏障

当前，数字经济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。数据要素作为数字经济深化发展的核心引擎，数据安全也成为事关国家安全和经济社会发展的重大议题。党中央、国务院高度重视数据安全工作，加快推动构建治理体系，筑牢安全基石。今年是党的二十大召开之年，也是实施“十四五”数字经济规划承上启下的重要一年，做好数据安全工作意义重大。

维护数据安全是顺应时势的必然选择

数据安全是数字经济发展的压舱石。发展数字经济是我国当前和今后的首要经济任务。我国陆续发布大数据战略、要素市场化配置等一系列政策，着力促进数据要素流通使用。数据大规模流通使用显著增加了数据触点和暴露面，数据泄露、滥用、垄断等风险问题日益凸显，据统计 2021 年全球数据泄露量高达 227.7 亿条。数据安全事件频发导致企业不敢、不

愿、不能共享数据，形成“信息孤岛”，从而制约数字经济发展活力与动力。调查显示有三成受访者完全不愿与智能网联汽车分享个人敏感信息。

数据安全是国家安全的重要组成部分。数据与国家经济运行、社会治理、公共服务、国防安全等方面密切相关，数据泄露、丢失和滥用将直接威胁国家安全和社会稳定。近年来针对重要行业与关键基础设施的数据攻击手段不断推陈出新，重要数据安全威胁加大。监测发现，46 个国家级 APT 组织中，绝大多数都以窃取其他国家政治、经济、军事和科技领域的数据为目标。尤其在地缘政治冲突下，数据安全已成为各国第一道防线。此次俄乌军事行动开始前，便爆发了针对乌克兰政府机构的大规模分布式拒绝服务攻击和数据擦除恶意软件攻击，导致大量重要数据泄露和丢失。

数据安全成为世界主要国家战略布局重点。世界主要国家和地区积极加强数据安全领域的前瞻性战略布局，兼顾国家安全与数字经济发展。欧盟发布《欧洲数据战略》及《数据治理法案》提案后，于 2022 年 2 月通过《数据法》草案，保障数据安全的同时，着力改善欧盟内部市场的数据共享机制，提升数据可用性和流动性，充分释放欧洲数字经济潜力。2019 至 2021 年，美国相继发布《联邦数据战略和 2020 年行动计划》《国防部数据战略》等战略文件，强调“将数据作为战略资源开发”，并采取严格措施保护国防等重要数据安全，构筑国家安全屏障。

我国数据安全管理进入落地实施阶段

数据安全法律框架初步形成。近年来，我国高度重视数据安全保护工作，在总体国家安全观的指引下，逐步完善数据安全法制版图。去年发布实施的《数据安全法》《个人信息保护法》，与《网络安全法》共同构成了我国数据安全立法的“三驾马车”，数据安全保护要求进一步明确。网信、工信、公安等传统涉网安全管理部门依职责率先推动制定配套立法，落实顶层法律中数据安全管理规定。上海、深圳、海南等 13 省市已制定本地区数据发展条例，探索数据要素流动共享安全规则。

数据安全监管实践有序推进。在数据利用过程中，违法违规收集个人信息、数据泄露滥用等问题较为突出。近年来，网信、公安、市场监管等部门普遍以专项行动为牵引，持续加大 APP 违法违规收集使用个人信息、数据非法获取和交易、“大数据杀熟”等重点热点问题整治。信息通信行业作为数字化转型的先驱，结合行业数据安全管理需求，积极推动行业企业落实数据安全保护责任，同时聚焦行业数据安全突出问题开展专项行动，数据违规共享、数据安全保障措施不到位等突出问题治理成效显著。

数据安全产业发展持续向好。在数据安全事件频发、合规监管趋严等多重背景下，数据

安全需求全面释放，数据安全产业发展迎来重大机遇，据估算 2021 年全球数据安全市场规模约为 190 亿美元，到 2027 年将达到 542.3 亿美元。我国数据安全产业发展势头更为强劲，典型安全企业数据安全产品收入增长率超 100%，咨询规划、评估测试等数据安全服务销售额增长达 50%。数据安全产品体系逐步完善，覆盖数据资产管理、共享流通安全、追踪溯源等数据全生命周期，产业支撑能力不断提升。

深入推进我国数据安全工作

制度先行，逐步完善配套法规政策体系。为贯彻落实数据安全相关立法，各行业各部门需要结合需求，配套制定相关法规政策，为落实法律要求提供细化指引。一是重点推进数据分类分级、数据出境管理、数据安全评估等关键制度实施细则。二是研究制定重要数据识别、保护要求、风险评估等配套指引，完善重要数据全流程安全保障体系。

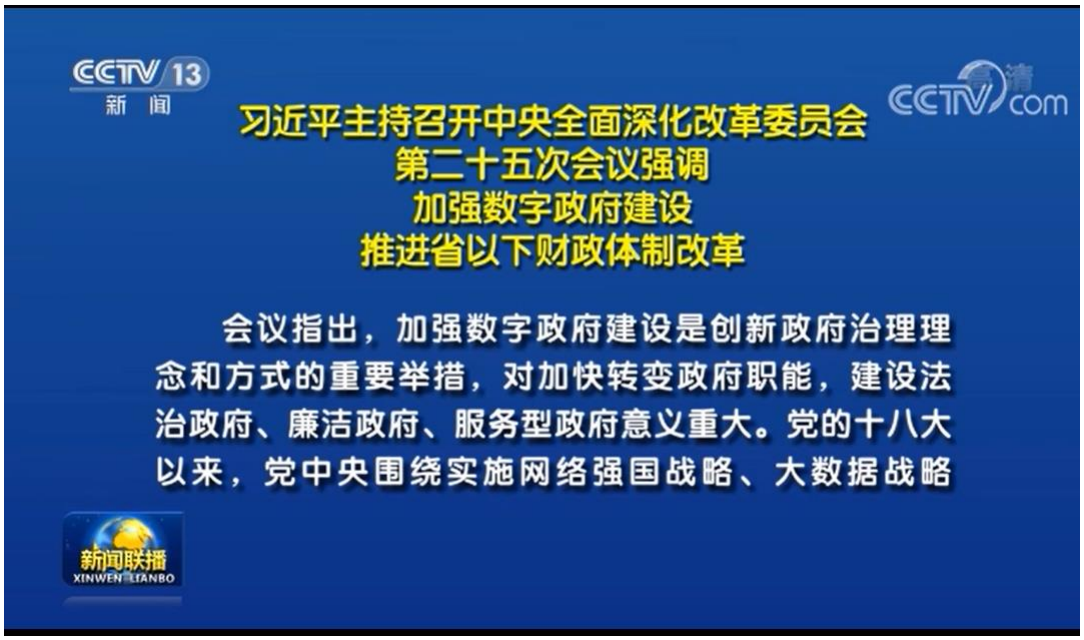
综合施策，持续提升企业数据安全保护水平。企业是数据安全保障的第一责任主体，推动企业落实主体责任，提升数据安全保障能力，可以有效防范化解安全风险。一是综合运用监督检查、贯标试点、评估检测等多种手段，引导企业提升数据安全保护水平。二是加快构建数据安全态势感知能力，加强数据安全风险监测和管理。三是开展重要数据安全风险评估，提升企业重要数据全生命周期安全风险防范能力。

创新引领，大力推动数据安全产业高质量发展。保障数据安全离不开数据安全技术和产业的有力支撑。作为新兴产业，发展数据安全产业需要产学研用协同创新。一是优化数据安全产业发展政策环境，依托专精特新、产融合作等多种政策，培育数据安全领军企业。二是采取“揭榜挂帅”等方式，鼓励数据安全关键技术攻关和产品孵化，通过示范引领推动数据安全技术产品的应用落地。三是建立行业数据安全人才培养体系，探索建设行业数据安全人才基地。（来源：人民邮电报）

四、政府之声

➢ 中央深改委审议通过《关于加强数字政府建设的指导意见》

2022 年 4 月 19 日，中共中央总书记、国家主席、中央军委主席、中央全面深化改革委员会主任习近平 4 月 19 日下午主持召开中央全面深化改革委员会第二十五次会议，审议通过了《关于加强数字政府建设的指导意见》、《关于进一步推进省以下财政体制改革工作的指导意见》、《关于建立健全领导干部自然资源资产离任审计评价指标体系的意见》、《“十四五”时期完善金融支持创新体系工作方案》、《关于完善科技激励机制的若干意见》。



会议指出，加强数字政府建设是创新政府治理理念和方式的重要举措，对加快转变政府职能，建设法治政府、廉洁政府、服务型政府意义重大。党的十八大以来，党中央围绕实施网络强国战略、大数据战略等作出一系列重大部署，各方面工作取得新进展。要把坚持和加强党的全面领导贯穿数字政府建设各领域各环节，坚持正确政治方向。要把满足人民对美好生活的向往作为数字政府建设的出发点和落脚点，打造泛在可及、智慧便捷、公平普惠的数字化服务体系，让百姓少跑腿、数据多跑路。要以数字化改革助力政府职能转变，统筹推进各行业各领域政务应用系统集约建设、互联互通、协同联动，发挥数字化在政府履行经济调节、市场监管、社会管理、公共服务、生态环境保护等方面职能的重要支撑作用，构建协同高效的政府数字化履职能力体系。要强化系统观念，健全科学规范的数字政府建设制度体系，依法依规促进数据高效共享和有序开发利用，统筹推进技术融合、业务融合、数据融合，提

升跨层级、跨地域、跨系统、跨部门、跨业务的协同管理和服务水平。要始终绷紧数据安全这根弦，加快构建数字政府全方位安全保障体系，全面强化数字政府安全管理责任。（来源：新华社）

- **全文：**http://www.gov.cn/xinwen/2022-04/19/content_5686128.htm

➢ 中办国办印发《关于加强打击治理电信网络诈骗违法犯罪工作的意见》

2022 年 4 月 18 日，中共中央办公厅、国务院办公厅印发了《关于加强打击治理电信网络诈骗违法犯罪工作的意见》（以下简称《意见》），对加强打击治理电信网络诈骗违法犯罪工作作出安排部署。


中华人民共和国中央人民政府
www.gov.cn
简 | 繁 | EN | 注册 | 登录
关于加强打击治理电信网络诈骗违法犯罪工作的意
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 > 新闻 > 滚动
中共中央办公厅 国务院办公厅印发《关于加强打击治理电信网络诈骗违法犯罪工作的意见》
2022-04-18 19:28 来源： 新华社
【字体：大 中 小】 打印
新华社北京4月18日电 近日，中共中央办公厅、国务院办公厅印发了《关于加强打击治理电信网络诈骗违法犯罪工作的意见》（以下简称《意见》），对加强打击治理电信网络诈骗违法犯罪工作作出安排部署。
《意见》强调，要坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻党的十九大和十九届历次全会精神，坚持以人民为中心，统筹发展和安全，强化系统观念、法治思维，坚持严厉打击、依法办案，实现法律效果与社会效果有机统一，坚持打防结合、防范为先，强化预警劝阻，加强宣传教育，坚持科技支撑、强化反制，运用科技信息化手段提升技术反制能力，坚持源头治理、综合治理，加强行业监管，强化属地管控，坚持广泛动员、群防群治，发动群众力量，汇聚群众智慧，坚决遏制电信网络诈骗违法犯罪多发高发态势，提升社会治理水平，使人民获得感、幸福感、安全感更加充实、更有保障、更可

《意见》要求，要构建严密防范体系。强化技术反制，建立对涉诈网站、APP 及诈骗电话、诈骗短消息处置机制；强化预警劝阻，不断提升预警信息监测发现能力，及时发现潜在受害群众，采取劝阻措施；强化宣传教育，建立全方位、广覆盖的反诈宣传教育体系，开展防范电信网络诈骗违法犯罪知识进社区、进农村、进家庭、进学校、进企业活动，形成全社会反诈的浓厚氛围。

《意见》要求，要加强行业监管源头治理。建立健全行业安全评估和准入制度；加强金融行业监管，及时发现、管控新型洗钱通道；加强电信行业监管，严格落实电话用户实名制；加强互联网行业监管；完善责任追究制度，建立健全行业主管部门、企业、用户三级责任制；

建立健全信用惩戒制度，将电信网络诈骗及关联违法犯罪人员纳入严重失信主体名单。《意见》还要求，要强化属地管控综合治理，加强犯罪源头地综合整治。

《意见》强调，各级党委和政府要加强对打击治理电信网络诈骗违法犯罪工作的组织领导，统筹力量资源，建立职责清晰、协同联动、衔接紧密、运转高效的打击治理体系。金融、电信、互联网等行业主管部门要全面落实行业监管主体责任，各地要强化落实属地责任，全面提升打击治理电信网络诈骗违法犯罪的能力水平。（来源：新华社）

- **全文：**http://www.gov.cn/xinwen/2022-04/18/content_5685895.htm

➢ 10 项网络安全国家标准获批发布

2022 年 4 月 15 日，国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告(2022 年第 6 号)，全国信息安全标准化技术委员会归口的 10 项国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	代替标准号	实施日期
1	GB/T 41387-2022	信息安全技术 智能家居通用安全规范		2022-11-01
2	GB/T 41388-2022	信息安全技术 可信执行环境 基本安全规范		2022-11-01
3	GB/T 41389-2022	信息安全技术 SM9 密码算法使用规范		2022-11-01
4	GB/T 41391-2022	信息安全技术 移动互联网应用程序（App）收集个人信息基本要求		2022-11-01
5	GB/T 41400-2022	信息安全技术 工业控制系统信息安全防护能力成熟度模型		2022-11-01
6	GB/T 41479-2022	信息安全技术 网络数据处理安全要求		2022-11-01
7	GB/T 20984-2022	信息安全技术 信息安全风险评估方法	GB/T 20984-2007	2022-11-01
8	GB/T 29829-2022	信息安全技术 可信计算密码支撑平台功能与接口规范	GB/T 29829-2013	2022-11-01
9	GB/T 30283-2022	信息安全技术 信息安全服务 分类与代码	GB/T 30283-2013	2022-11-01
10	GB/T 31506-2022	信息安全技术 政务网站系统安全指南	GB/T 31506-2015	2022-11-01

（来源：全国信息安全标准化技术委员）

- **全文：**https://www.tc260.org.cn/front/postDetail.html?id=20220424092126

➢ 证监会就《证券期货业网络安全管理办法（征求意见稿）》公开征求意见

2022 年 4 月 29 日，为建立健全证券期货业网络安全监管制度体系，防范化解行业网络安全风险隐患，维护资本市场安全平稳高效运行，证监会起草了《证券期货业网络安全管理办法(征求意见稿)》(以下简称《办法》)，现向社会公开征求意见。

《证券期货业网络安全管理办法(征求意见稿)》共八章六十六条：主要包括证券期货业网络安全监督管理体系、网络安全运行、数据安全统筹管理、网络安全应急处置、关键信息基础设施网络安全、网络安全促进与发展、监督管理与法律责任等方面内容。具体内容详见《办法》起草说明。欢迎社会各界对《办法》提出宝贵意见，证监会将根据公开征求意见情况，进一步完善《办法》并履行程序后发布实施。（来源：证监会）

- **《证券期货业网络安全管理办法（征求意见稿）》**
- **全文：**http://www.csrc.gov.cn/csrc/c101981/c2381308/content.shtml

五、本期重要漏洞实例

➢ Microsoft 发布 2022 年 4 月安全更新

发布日期：2022-4-12

更新日期：2022-4-12

描述：2022 年 4 月 12 日，微软发布了 2022 年 4 月份的月度例行安全公告，修复了多款产品存在的 103 个安全漏洞。受影响的产品包括：Windows 11（69 个）、Windows Server 2022（98 个）、Windows 10 21H2（72 个）、Windows 10 21H1（72 个）、Windows 10 20H2 & Windows Server v20H2（97 个）、Windows 8.1 & Server 2012 R2（63 个）、Windows Server 2012（57 个）、Windows RT 8.1（47 个）和 Microsoft Office-related software（4 个）。利用上述漏洞，攻击者可以绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CVE 编号	公告标题	最高严重等级和漏洞影响	受影响的软件
CVE-2022-26809	Remote Procedure Call Runtime 远程代码执行漏洞	严重 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-24491	Windows Network File System 远程代码执行漏洞	严重 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-24541	Windows Server Service 远程代码执行漏洞	严重 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1

CVE-2022-24500	Windows SMB 远程代码执行漏洞	严重 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-23257	Windows Hyper-V 远程代码执行漏洞	严重 远程代码执行	Windows 11 Server 2022 Windows 10 Server, version 20H2
CVE-2022-24487	Windows Local Security Authority (LSA) 远程代码执行漏洞	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016
CVE-2022-24533	Remote Desktop Protocol 远程代码执行漏洞	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-24521	Windows Common Log File System Driver 权限提升漏洞	重要 特权提升	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-26904	Windows User Profile Service 权限提升漏洞	重要 特权提升	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2

			Server 2012 Windows 8.1

来源：https://msrc.microsoft.com/update-guide/releaseNote/2022-Apr

➢ Oracle MySQL Server 输入验证错误漏洞

发布日期：2022-04-19
更新日期：2022-04-29
受影响系统：
Oracle Oracle MySQL Server <= 8.0.28
描述：

CVE(CAN) ID: CVE-2022-21425
Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。MySQL Server 是其中的一个数据库服务器组件。
Oracle MySQL Server（组件：Server: DDL）8.0.28 及之前版本存在输入验证错误漏洞。未经身份验证的攻击者可利用该漏洞通过多种协议进行网络访问，从而破坏 MySQL Server，导致 MySQL Server 挂起或频繁崩溃（拒绝服务）及对 MySQL Server 某些可访问数据进行未授权更新、插入或删除。
链接：https://www.oracle.com/security-alerts/cpuapr2022.html
建议：

厂商补丁：
Oracle
Oracle 已经为此发布了一个安全公告（cpuapr2022）以及相应补丁：
cpuapr2022：Oracle Critical Patch Update Advisory - April 2022
链接：https://www.oracle.com/security-alerts/cpuapr2022.html

➢ IBM QRadar SIEM 身份验证错误漏洞

发布日期：2022-04-25
更新日期：2022-04-29
受影响系统：
IBM IBM QRadar SIEM 7.5
IBM IBM QRadar SIEM 7.4
IBM IBM QRadar SIEM 7.3
描述：

CVE(CAN) ID: CVE-2021-38878
IBM QRadar SIEM 是美国 IBM 公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。该方

案提供对整个 IT 架构范围进行监督、生成详细的数据访问和用户活动报告等功能。
IBM QRadar SIEM 7.3、7.4 和 7.5 版本存在身份验证错误漏洞，该漏洞源于身份验证错误。攻击者可利用该漏洞冒充用户。
建议：

厂商补丁：
IBM

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://www.ibm.com/support/pages/node/6574787

➢ Google Android 权限提升漏洞

发布日期：2022-01-14
更新日期：2022-04-27
受影响系统：
Google Google Android
描述：

CVE(CAN) ID: CVE-2021-39684
Google Android 是美国谷歌（Google）公司的的一套以 Linux 为基础的开源操作系统。
Google Android 内核的 Bootloader 组件存在权限提升漏洞，该漏洞源于代码中的逻辑错误。攻击者可利用该漏洞在无需其他执行权限的情况下提升本地权限。
<*链接：https://source.android.com/security/bulletin/2022-01-01
建议：

厂商补丁：
Google

Google 已经为此发布了一个安全公告（2022-01-01）以及相应补丁：
2022-01-01：Android Security Bulletin—January 2022
链接：https://source.android.com/security/bulletin/2022-01-01

六、本期网络安全事件

➢ 因网络安全事件 招商证券遭深圳证监局责令整改

2022 年 3 月 14 日交易系统出现故障后，变更管理不完善，应急处置不及时、不到位，招商证券日前被深圳证监局采取责令改正监管措施。

繁體 | 无障碍

中国证券监督管理委员会 CHINA SECURITIES REGULATORY COMMISSION 深圳监管局

敬畏市场、敬畏法治、敬畏专业、敬畏风险、发挥合力

请输入关键字

首页 | 证监局介绍 | 辖区监管动态 | 政务信息 | 办事服务 | 辖区数据 | 互动交流 | 专题专栏

当前位置：首页 > 政务信息 > 主动公开目录 > 证监局主题分类 > 行政执法

索 引 号	bm56000001/2022-00003756	分　类	行政执法;行政监管措施
发布机构		发文日期	2022年04月02日
名　称	深圳证监局关于对招商证券股份有限公司采取责令改正措施的决定		
文　号	行政监管措施决定书(2022)47号	主 题 词	

深圳证监局关于对招商证券股份有限公司采取责令改正措施的决定

招商证券股份有限公司：

经查，你公司在2022年3月14日的网络安全事件中，存在变更管理不完善，应急处置不及时、不到位等问题。上述行为违反了《证券期货业信息安全保障管理办法》（证监会令第82号，以下简称《信息安全保障管理办法》）第二十二条、第三十二条第一款以及《证券基金经营机构信息技术管理办法》（证监会令第179号，以下简称《信息技术管理办法》）第二十二条第一款、第三十六条、第四十二条的相关规定。

深圳证监局明确整改要求

据深圳证监局官网消息：经查，招商证券在 2022 年 3 月 14 日的网络安全事件中，存在变更管理不完善，应急处置不及时、不到位等问题。上述行为违反了《证券期货业信息安全保障管理办法》第二十二条、第三十二条第一款以及《证券基金经营机构信息技术管理办法》第二十二条第一款、第三十六条、第四十二条的相关规定。依据《信息安全保障管理办法》第五十条，《信息技术管理办法》第五十七条，以及《证券期货业网络安全事件报告与调查处理办法》第二十八条的规定，深圳证监局决定对招商证券采取责令改正的行政监管措施。

深圳证监局表示，招商证券应进一步加强重要信息系统建设的统筹规划，充分了解系统架构及内部运行机制，强化研发、测试、上线、升级变更及运维管理，完善应急处置机制，保障关键岗位人员的专业能力和数量配置，确保信息系统安全平稳运行;同时招商证券应对此次事件相关责任人员进行内部责任追究。招商证券应于 3 个月内完成上述整改工作并向深圳证监局报送整改报告。

一度登上微博热搜

3 月 14 日，沪深两市开盘后，有投资者在社交平台反映，招商证券交易系统出现系统

故障，包括交易页面无法成交、无法撤回等问题。“招商证券崩了”当日上午登上了微博热搜。3 月 15 日，招商证券通过微信公众号发布了关于集中交易系统故障的情况说明。招商证券称，3 月 14 日，公司集中交易回报系统出现处理延迟等故障，导致部分客户未及时收到成交回报信息、撤单交易受影响。

法律人士表示，这件事给券商敲响了警钟，技术层面的安全保障永远在路上。券商应该切实履行好对投资者的安全保障义务，维护投资者的安全保障权，不断提升投资者的获得感和安全感，持续提升投资者信心。（来源：证券时报）

➢ 上市公司遭遇电信诈骗 大亚圣象子公司被骗 2275 万

2022 年 4 月 5 日，大亚圣象(000910)日前披露 2021 年度业绩报告显示，报告期内，公司全资子公司圣象集团有限公司下属子公司美国 HomeLegendLLC 公司成为一起电信欺诈的受害者，肇事者入侵该公司租用的微软公司 365 邮箱系统，伪造假电子邮件冒充该公司管理层成员，伪造供应商文件及邮件路径，实施诈骗，涉案金额约 356.9 万美元(折合人民币 2275.49 万元)。大亚圣象表示，该公司已于美国地方联邦执法当局备案并向中国公安机关报案，截至报告日，被盗资金追回可能性较低。

五、非主营业务分析

√ 适用 □ 不适用

单位：元

	金额	占利润总额比例	形成原因说明	是否具有可持续性
投资收益	26,102,416.58	3.49%	购买理财产品收益 901.58 万元，出售瑞晟公司股权收益 1,722.59 万元	否
资产减值	-12,065,776.36	-1.61%		
营业外收入	13,676,720.82	1.83%		
营业外支出	28,302,628.16	3.79%	美国 HomeLegendLLC 公司涉及 356.9 万美元诈骗损失	
其他收益	88,147,590.01	11.79%	本期收到增值税即征即退款 4,931.92 万元，其他政府补助 3,882.84 万元	扣除增值税即征即退款其他无可持续性

大亚圣象主要从事地板和人造板的生产销售业务，公司曾在投资者互动平台表示，公司木地板的市场占有率稳居行业首位，2021 年度公司地板销量为 6289 万平方米，被称为“地板大王”。2021 年公司营收 87.5 亿元，同比上升 20.46%;归属上市公司股东净利润 5.95 亿元，同比下降 4.86%;归属上市公司股东的扣非净利润为 5.57 亿元，同比下降 7.04%。

大亚圣象遭遇诈骗，在一定程度上说明大亚圣象的财务管理、安全保障方面存在缺陷。那么应该如何避免被骗呢?骗子的目的是骗钱，最终要通过转账的形式，达到骗取钱财的目的，所以无论骗子如何花言巧语、危言恐吓大家一定要记住“不听、不信、不转账、不汇款”有疑问直接拨打 110 进行咨询或报警。

以下是总结的 9 大防骗“秘籍”：

1.短信内链接都别点：虽然手机短信中也有银行等机构发来的安全链接，但不少用户难以通过对方短信号码、短信内容、链接形式等辨别真伪，所以建议用户尽量不要点击短信中自带的任何链接。特别是 Android 手机用户，更要防止中木马病毒。2.“验证码”谁都别给：银行、支付宝等发来的“短信验证码”是极其隐秘的隐私信息，且通常几分钟之后即自动过期，所以不要向任何人和机构透露该信息。3.手机不显号码，别接：目前，除极少数特殊部门还拥有“无显示号码”电话之外，任何政府、企业、银行、运营商等机构均没有“无显示号码”的电话，所以今后再见到“无显示号码”来电，直接挂断就好。4.闭口不谈卡号和密码：对话中都绝不提及银行卡号、密码、身份证号码、医保卡号码等信息，以免被诈骗分子利用。5.钱财只能进不能出：任何要求自己打款、汇钱的行为都得长心眼，警方建议如需打款可至线下银行柜台办理，如心中有疑惑，可向银行柜台工作人员咨询。6.陌生证据莫轻信：由于个人隐私泄露泛滥，诈骗分子常常会掌握用户的一些个人信息，并以此作为证据，骗取用户信任，此时切记要多长个心眼——绝不轻易相信陌生人，就算朋友家人，如果仅仅是在网上，也不可轻信。7.钓鱼网站要提防：切不可轻易信任那些看上去与官方网站长得一模一样的钓鱼网站，中病毒不说，还可能被直接骗走钱财，所以在登录银行等重要网站时，养成核实网站域名、网址的习惯。8.新鲜事要注意：诈骗分子常常利用最新的时事热点设计骗局内容，如房产退税、热播电视节目等都常常被骗子利用。如果不明电话中提及一些你从未接触过的新鲜事，也切莫轻易当真。9.拿不准就打 110：如果真有拿不准的事，拨打 110 无疑是最可靠的咨询手段，虽然麻烦了警察，但必要时候仍可以采取这种手段。（来源：每日经济新闻）

➢ 华为员工利用公司系统 Bug 越权访问机密数据被判刑

2022 年 4 月 12 日上午消息，与华为员工有关的一件案子日前浮出水面。该判决实际上早在去年 9 月就做出，今年 2 月 16 日公开发布在了裁判文书网，并于近日被媒体曝光。案

件案号为(2021)粤 03 刑终 1657 号，题为《易某非法获取计算机信息系统数据、非法控制计算机信息系统刑事二审刑事裁定书》。

简单来说，案件涉及的华为员工易某调离岗位后未清理 ERP 登陆信息，利用 bug 越权访问，将获得数据透露给第三方获利。最终被判犯非法获取计算机信息系统数据罪，判处有期徒刑一年，并处罚金人民币二万元;并向易某追缴违法所得共计人民币 23437.6 元，依法予以没收，上缴国库。

2010 年 12 月，易某从华为公司线缆物控部调任后，未按华为公司的要求将 ERP 账户线缆类编码物料价格的查询权限清理，至 2017 年底，易某违反规定多次通过越权查询、借用同事账号登录的方式在 ERP 系统内获取线缆物料的价格信息。2017 年以后，易某发现 ERP 系统中的 POL 采购小程序存在漏洞，能通过特定操作绕过权限控制查看系统数据，便以此方式获取线缆物料的价格信息。易某将非法获取的价格数据以发短信、打电话、发电子邮件的方式告知深圳市金信诺高新技术股份有限公司(华为技术有限公司的供应商)，从而帮助金信诺公司在华为公司的招标项目中提高中标率。

在 2016 年 12 月 27 日至 2018 年 2 月 28 日期间，多次通过公司邮箱将华为多个供应商共 1183 个(剔除重复部分共 918 个)线缆类编码物料的采购价格发送给金信诺公司。其在 2012 年至 2017 年 6 月 30 日期间，收受金信诺公司购物卡共计 7000 元、篮球鞋 5 双(价值共计人民币 16437.6 元)。案发后，华为公司出具谅解书，表示对易某侵害华为公司的行为予以谅解。一审后，易某提起上诉，请求撤销原审判决，并依法改判为免于刑事处罚。法院二审驳回上诉，维持原判。（来源：IT 之家）

➢ 因售卖公民个人信息 两航空公司客服人员获刑并被“禁业”

2022 年 4 月 22 日，粉丝追星买卖航班行程轨迹，四人被诉侵犯公民个人信息罪。北京市朝阳区人民法院对这起案件作出一审判决。

徐某与张某，是热衷追星的“粉丝”，两人为了拉近与偶像的距离，找到了来自不同航空公司的客服人员秦某与李某。通过他们，两位“粉丝”多次购买明星的航班轨迹等信息。秦某与李某利用职务之便，将包含航班轨迹、公务舱舱单等在内的公民个人信息进行贩卖，获利六万余元。检察机关指控，四名被告人非法获取、提供公民个人信息，应当以侵犯公民个人信息罪追究其刑事责任。考虑到出售公民信息的行为同时侵害了社会公共利益，检方对被告人秦某、李某同时提起附带民事公益诉讼。这起案件于 2022 年 3 月 31 日在北京市朝阳区人民法院公开审理。4 月 22 日，法院作出一审判决。

法院审理认为，被告人秦某伙同李某，出售公务舱舱单以及其他公民个人信息数千条，情节特别严重。被告人徐某与张某为了满足自己追星的目的，非法获取公民个人信息，情节严重。被告人秦某、李某均构成侵犯公民个人信息罪，分别被判处有期徒刑三年，并处罚金人民币四万元。同时，秦某、李某三年内被禁止从事航空客服代表类职业。被告人张某被判处有期徒刑一年，缓刑一年，并罚金人民币一万元;被告人徐某被判处拘役五个月，缓刑五个月，并处罚金人民币五千元。

针对检察机关提起的民事公益诉讼，北京市朝阳区人民法院也作出了判决：责令被告

秦某、李某共同支付公共利益损害赔偿款四万余元;责令被告秦某支付公共利益损害赔偿款六千两百余元，被告李某支付公共利益损害赔偿款一万八千余元;责令两人注销买卖公民个人信息使用的微信号，删除存储在其中的公民个人信息数据，并在国家级新闻媒体就侵犯公民个人信息行为向社会公众公开赔礼道歉。（来源：央视新闻）

➢ 哥斯达黎加政府部分网络系统因遭黑客攻击 仍处于关闭状态

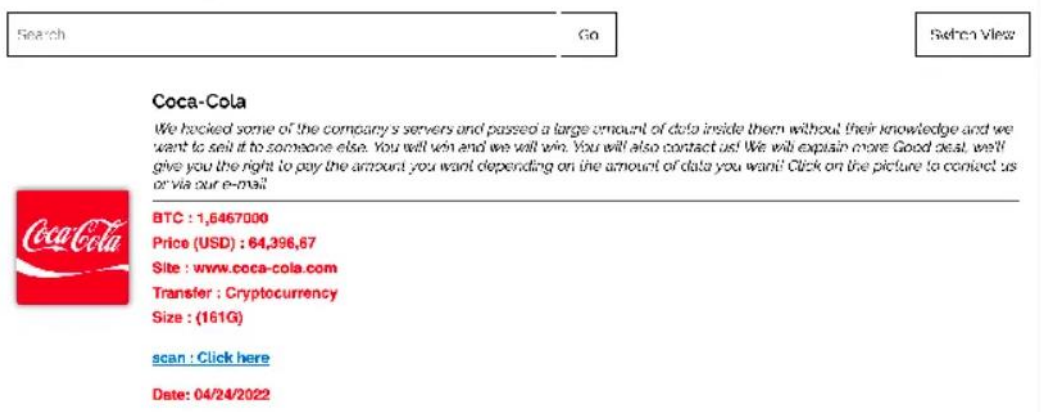
2022 年 4 月 22 日，截至当地时间因遭到国际黑客攻击，哥斯达黎加部分政府公共服务网络仍处于关闭状态。哥斯达黎加总统阿尔瓦拉多此前一天对此表示谴责。他表示，哥斯达黎加不会向国际黑客组织妥协，目前有关部门正在加紧网络管理技术升级，加固网络安全，同时评估泄漏数据的规模和损失，与国际组织和公司合作，加紧恢复受损系统。

当地时间 18 日，哥斯达黎加财政部的网络系统就遭到黑客攻击，政府随即采取预防性措施，关闭了部分系统。该国养老金、公共系统薪酬支付以及税收、进出口系统均受到不同程度影响。

据当地媒体报道，目前已有包括社会保障、劳工部等在内的至少 6 个政府部门的网络系统遭到了黑客攻击。（来源：央视新闻）

➢ 可口可乐遭黑客入侵 161GB 数据被窃取 官方称正在调查

2022 年 4 月 29 日，据 The Register 报道，跨国碳酸软饮料品牌可口可乐被一个名为 Stormous 的黑客组织入侵。Stormous 在暗网上列出了大约 161GB 的可口可乐数据。清单上写着：“我们入侵了可口可乐的一些服务器，并在他们不知情的情况下拿到了大量数据，打算进行出售”。



黑客要价为 1.6 个比特币(约 6.4 万美元)，它还补充说，价格可以“取决于你想要的数据量”进行协商。据了解，数据是在 2022 年 4 月 24 日泄露的，当时可口可乐官方就发布了声明。可口可乐通信全球副总裁 Scott Leith 告诉 The Register：“我们知道这件事，并正在调查以确定索赔的有效性。我们正在与执法部门协调。”

值得一提的是，黑客攻击前几天，Stomrous 在其 Telegram 群组上进行了一项调查，询问关注者要黑哪个公司，可口可乐获得了约 72%的投票。近日，可口可乐公开了今年第一季度的财报，数据显示其营收同比增长 16%，达到了 104.91 亿美元，高于外界预期的 98.3 亿美元。截至 4 月 27 日，可口可乐的股价在今年已经上涨了 11.55%。（来源：安全学习那些事儿）

信息安全意识产品服务

021-33663299