国盟信息安全通报

2021 年 05 月 31 日第 239 期

全国售后服务中心

国盟信息安全通报

（第 239 期）

国际信息安全学习联盟

2021 年 5 月 31 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 581 个，其中高危漏洞 120 个、中危漏洞 374 个、低危漏洞 87 个。漏洞平均分值为 5.40。本周收录的漏洞中，涉及 0day 漏洞 323 个（占 56%），其中互联网上出现“OpenEMR 操作系统命令注入漏洞、PHPGurukul Online Book Store 任意文件上传漏洞”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 3079 个，与上周（2544 个）环比增加 21% 。

主要内容

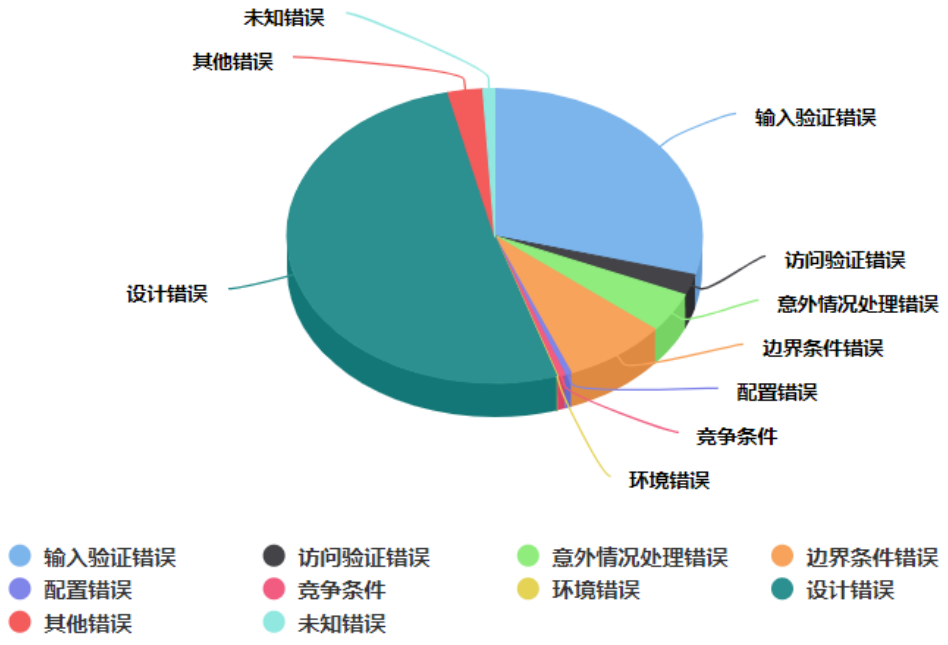
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

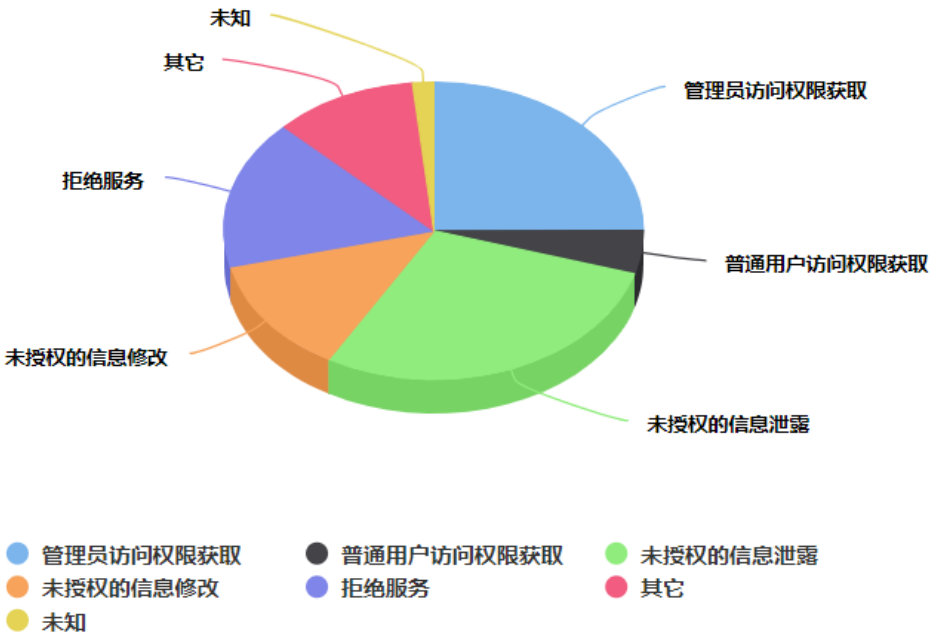
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 581 个，其中高危漏洞 120 个、中危漏洞 374 个、低危漏洞 87 个。漏洞平均分值为 5.40。本周收录的漏洞中，涉及 0day 漏洞 323 个（占 56%），其中互联网上出现“OpenEMR 操作系统命令注入漏洞、PHPGurukul Online Book Store 任意文件上传漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3079 个，与上周（2544 个）环比增加 21% 。

二、安全漏洞增长数量及种类分布情况

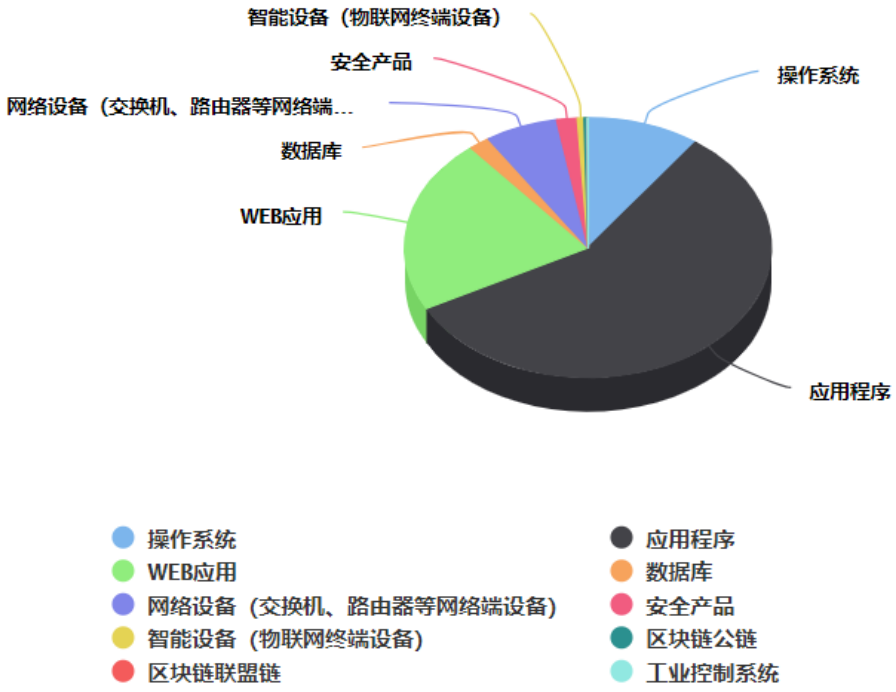
➢ 漏洞产生原因（2021 年 5 月 1 日—2021 年 5 月 31）



➢ 漏洞引发的威胁（2021 年 5 月 1 日—2021 年 5 月 31）



➢ 漏洞影响对象类型（2021 年 5 月 1 日—2021 年 5 月 31）



三、安全产业动态

➢ 以自主创新推进网络强国建设的科学指南

党的十八大以来，以习近平同志为核心的党中央高度重视网信事业发展，准确把握发展大势，站在历史和全局的高度，围绕网络安全和信息化领域重大问题，周密部署、科学决策，提出一系列新思想新观点新论断，不断推进理论创新与实践创新，坚定不移地走出一条中国特色治网之道，形成了网络强国战略思想。《习近平关于网络强国论述摘编》一书收录了习近平总书记关于自主创新推进网络强国建设的重要论述，系统深入地阐释了网络强国战略思想的丰富内涵，科学地回答了为什么建设网络强国、建设什么样的网络强国、怎样建设网络强国的时代课题，为新时代把握信息革命重大历史机遇、做大做强网信事业、加快推进网络强国建设提供了根本遵循和科学指南，是指导新时代网络安全与信息化发展的纲领性文献。

抢抓发展机遇，走出一条中国特色治网之道

习近平总书记强调：“信息化为中华民族带来了千载难逢的机遇。”人类社会先后经历了农业革命、工业革命，当前，正在经历由信息技术和数字技术为代表的信息革命。互联网是信息革命的产物，是深刻影响当今世界的颠覆性力量，也是最大变量，信息化越来越成为推动经济社会发展的主要动力，面对风云诡谲的国际竞争，谁能在信息革命中抢抓先机，谁就能牢牢掌握时代的主动权，赢得全方位综合国力的竞争。十八大以来，以习近平同志为核心的党中央攻坚克难、锐意进取，中国经济实现“弯道超车”，成为世界第二大经济体。信息化浪潮带来的新一轮科技革命、产业变革和信息革命，正值中国特色社会主义进入新时代，中华民族前所未有地走向世界舞台的中心，前所未有地接近民族复兴的伟大目标，前所未有地拥有实现这一目标的信心、决心和能力，同时，与中国加快转变经济发展方式的时机相契

合，为我们自主创新谋发展、牢牢掌握网络意识形态主导权、完善和发展中国特色社会主义制度、拓展中国特色社会主义道路提供了难得的重大机遇。必须抢先一步，紧紧抓住并用好这一千载难逢的机遇，自主创新走中国特色治网之道。

习近平总书记明确提出：“要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。”其中，“多主体参与”与“多种手段相结合”之“两多”，处处体现中国特色，实为中国特色治网之道。网络空间虽是虚拟的，但经营网络空间、在网络空间活动的各主体却是现实、多元的，用网管网治网也需要技术、法律、经济等多种手段保驾护航，营造风清气正的网络空间、实现网络安全和信息化双轮驱动，是一项艰巨复杂的系统工程。首先，要推动网络治理的全方位联动。加强党的集中统一领导，明确党政的管理责任，各级党委和领导干部要严格落实一把手责任制，做到人人有责、人人尽责，切实增强治网管网的责任心和使命感；压实互联网企业的主体责任，加强互联网行业自律，把好网络信息安全关口，决不能让有害信息在网络空间泛滥，决不能姑息别有用心之人利用网络平台造谣生事；动员广大网民厚植家国情怀，增强网络道德自觉，主动参与、积极配合网络治理。其次，要加强网上正面宣传。积极发挥互联网的舆论引导功能，在创新网络宣传理念、内容、形式、方法、手段上下功夫，推进网络媒体与传统媒体深度融合，实现网上网下同频共振，以大众喜闻乐见的方式讲好中国故事，在润物无声中让习近平新时代中国特色社会主义思想和十九大精神入脑入心，让共产主义崇高理想和坚持中国特色社会主义的强大信念成为社会共识，让核心价值观成为人民价值取向的最大公约数，最大程度巩固全党全人民团结奋斗的思想基础。最后，要维护好网络安全。树立正确的网络安全观，充分认识网络安全之于国家安全的重要位置，充分认识网络安全动态、开放、相对的发展实际，加强网络安全知识技能宣传普及，提高广大网民的网络安全自觉和自我防护技能，引导各方力量共筑网络安全防护网；积极发展网络安全产业，加快构建关键信息基础设施防护体系，落实行业、企业的主体防护责任和主管部门的监管责任，建立统一高效的网络安全分析、研判、预警机制和重大事件协调、处理机制，提升网络安全实践应急指挥能力，做到关口前移、防患未然；依法严厉打击网络违法犯罪行为，维护民众合法权益，增强网络安全防御威慑力。

践行新发展理念，释放网信事业巨大潜能

当今世界，信息技术革命大潮风起云涌，中国经济发展进入新常态，新常态需要新动力，网信事业大发展成为完善和发展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的新契机。习近平总书记作出明确要求：“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，围绕建设现代化经济体系、实现高质量发展，加快信息化发展，整体带动和提升新型工业化、城镇化、农业现代化发展。”

自主创新是推动发展的动力源泉。习近平总书记多次强调，“核心技术是国之重器”，互联网核心技术是我们最大的“命门”，“命门”掌握在别人手里是最大的隐患，而打开“命门”的“钥匙”就是自主创新，下定决心、保持恒心、找准重心，加快信息领域核心技术突破。十八大以来，以习近平同志为核心的党中央，先后周密部署创新驱动发展战略、信息化发展战略、国家“大数据”战略、“互联网+”行动计划，在数字产业化方面取得了举世瞩目的成就。在实现“两个百年”奋斗目标的紧要关头，更要坚定不移实施创新驱动战略，进一步释放数字经济发展的放大、叠加、倍增作用，推动互联网、大数据、人工智能等信息技术和实体经济的深度融合，不断催生数字经济新产业新业态新模式，加快各行业数字化、网络化、智能化进程，加速中国现代化经济体系的建设步伐。协调是健康、有序、可持续发展的内在要求。要着力解决网信事业发展中的不协调、不平衡问题，加强农村特别是偏远地区基础设施建设缩小城乡差异和地区差异；努力消除数字鸿沟，扩大公共基础服务的覆盖面，优化服务流程。此外，互联网企业发展要兼顾经济效益和社会效益，坚持自身发展和自觉履责并重，把好网络信息安全关口，发挥好互联网引导舆论、服务民众的效能。绿色是人民追求美好生活的重要指针，也是永续发展的前提。网络信息化产业本身自带低碳、环保的绿色属性，产业数字化以全方位、全角度、全链条地推动着工业、农业、国防、公共服务等各领域的改造和升级，加快促进绿色生产方式和生活方式的形成和发展。同时，网信事业自身也要实现绿色发展，旗帜鲜明地坚持正确政治方向、舆论导向、价值取向，营造风清气正的网络空间，维护好亿万民众共同的精神家园。开放是发展的必经之路。网络空间是无国界的，网络空间的发展与治理理应由世界各国人民共同掌握，要以开放的姿态迎接世界信息技术革命的洗礼，积极参与国际网络空间治理与合作，助力构建和平、民主、透明、合作、安全的全球互联网治理体系。共享是发展的最终旨归。建设网络强国、发展信息化的出发点和落脚点是增进人民福祉，要时刻以人民为中心，发展为了人民、依靠人民，成果由人民共享，加强基础设施建设，加快全民普及互联网步伐，提升互联网服务大众水平，引导民众知网、懂网、用网、护网，通过互联网了解世界、交流文化、创新创业、改善生活，增强获得感、幸福感、安全感。

加强党的集中统一领导，夯实网信事业发展之基

应对风云变幻的国际互联网发展大势，在互联网这个战场上打得赢、顶得住，做大做强网信事业，建设网络强国，关键在加强党的集中统一领导，确保网信事业始终沿着正确的方

向前进。

打铁还需自身硬。习近平总书记强调：“过不了互联网这一关，就过不了长期执政这一关。”各级党委是推动网信事业发展的掌舵人，要高度重视网信工作，加强组织领导，将网信工作纳入重点工作计划和议事日程，明确工作责任，确保责任到人，真正把工作落到实处；不断改革、完善党对网信工作的管理方式、机制体制，把握好时度效，全面提升解决新情况新问题的能力。各级领导干部特别是高级干部要站在党接受长期执政考验、巩固执政地位、提高执政能力的高度，以强烈的使命感和责任感，强化互联网思维，积极主动适应信息化带来的新要求，加强学习、努力探索，力求准确把握互联网发展规律、有效引导网络舆论、稳步驾驭信息化发展、切实保障网络安全，从容面对机遇和挑战；要坚持走网上群众路线，善于运用多种手段在互联网上组织群众、宣传真理、引导舆论、开展服务，不断提高执政能力。此外，还要全面从严打造网信管理人才队伍。要确保网信事业沿着正确方向前进，就必须把讲政治作为选拔网信人才的首要条件。要不断增强“四个意识”，始终把党的政治建设摆在首位，自觉维护党中央集中统一领导，把政治觉悟高、业务能力强、敢于担当、善于创新作为重要标准来打造强健的网信队伍，为网信事业发展提供坚实的组织保障。此外，网信事业具有技术密集属性和创新驱动属性，必须择天下英才以用之，要优化网信人才培养、引进、使用体制机制改革，构建具有核心竞争力的人才制度体系，释放广大英才的聪明才智和创新活力。（来源：人民论坛网）

➢ 赵泽良：规范引导数字平台健康发展是时代面临的新课题

日前，中央网信办副主任、国家网信办副主任赵泽良出席在杭州举办的 2021 西湖论剑·网络安全大会，并针对“安全是数字化改革之根基”这一话题分享了自身的看法和见解。

赵泽良表示，当今数字化、网络化、智能化已经成为时代特征和发展趋势，数字化、网络化、智能化在极大促进经济和社会的发展，但与此同时，数字化发展也为民众生活带来了不容小觑的安全风险和挑战。他认为，面对数字化带来的风险和隐患，国家有关的监管机构和社会企业都应该积极探索如何推动人工智能、物联网、下一代网络等新技术的应用，同时规范和引领新技术应用的问题。

赵泽良谈到，发展数字经济首先要准确把握数字平台的属性与定位。大型数字平台是数字经济发展的重要形式和载体，如今所有的平台都是数字平台，都具有数据的属性，由于数据平台的网络效应、对数据的虹吸效应以及边际成本趋于零的特性，平台的数据集中化已经成为了一个趋势，也容易发展成为一家独大的垄断式现象。这些数字化平台的公共空间属性、基础设施属性已经逐渐凸显出来，如何在大力支持平台发展的同时，让这些平台更规范、更健康，是当今时代面临的新课题，需要各界共同探讨、认真研究。

从数据与监管的角度来看，数字平台中的数据需要科学的分类与管理。数字平台上存储了海量的信息数据，其中既有用户的个人信息，也有公共信息，也有个人的通信数据，也有公共传播的数据。赵泽良认为，数字平台从设计之初就应该综合考虑个人信息、公共通信、个人数据和公共数据的分级分类管理，对个人信息严格保护，对公共数据加强监管、合理利用。从而逐渐形成具体的规则和标准，以及有效的安全监管体系。

从责任的角度来看，数字平台的责任界定应该更合理、明确。赵泽良表示，落实、夯实企业的网络安全主体责任，平台的网络安全责任已经是一个老生常谈的话，平台的网络安全责任，不应该仅仅是平台上的用户受到损害以后平台应该承担的责任，也不仅限于平台对平台上的违法有害信息应有监管责任。平台的网络安全责任还应在平台的设计过程中，在平台的严防过程中，在平台的各类功能设计上，在平台的体系结构上，都要以人民为中心，从用户的角度出发。

之所以近年来个人隐私安全问题日益突出，这背后不仅仅是个人隐私保护的问题，也是

企业商业模式，以及一个平台的应用模式的问题。现在将个人信息、个人隐私去货币化，商业化已成为一种商业模式，对个人信息、个人隐私的营销应该有规则、有监管，数字平台在设计之初就不应该仅仅考虑商业问题，还应考虑社会责任，考虑用户的利益，要保障和维护用户在平台上与网络空间的合法权益，落实平台的责任。甚至个人信息保护还应体现在平台社区规则上，每个平台都应该设计更合理的隐私政策和自己的用户规则，这一套社会规则、平台规则将在平台治理中发挥十分重要的作用。

“现在不少平台的隐私政策、使用规则不仅内容繁长，而且基本是偏向平台企业这一方，用户的利益难以得到保障。究其原因，还是要看这些规则的制定过程中有没有体现科学性，有没有体现民主性。有没有让广大的用户来深入参与，平台规则管理的是用户，而平台的用户实际上就相当于我们的公民，平台对用户的管理实际上是在对社会进行管理。”赵泽良讲道。

用于这些管理的规则就应有一套科学、民主、透明的程序，让社会来监督，让网民来参与，让政府来监管，只有这样我们才能把平台的责任，把企业的责任落到实处。

此外，数字化发展还要不断创新网络安全的方式方法。赵泽良谈到，今天的网络安全已不仅是数据的安全，或是系统的安全，而是越来越多地牵涉到我们控制系统的安全。随着新能源汽车、辅助驾驶汽车、无人驾驶汽车的发展，这一类安全问题更加突出。

经过过去多年的实践，网络安全行业已经形成了一套比较完备、也比较行之有效的网络安全的模式、策略和方法，但这一套安全的体系对车联网、智能驾驶、无人机等等新生的控制系统是否有效？还有哪些地方需要优化和完善？这些问题需要安全从业者们持续思考和反思。

当今大家都已经习惯了使用智能手机，如果手机上的某一个应用程序出了问题，很容易就可以打个补丁更新，甚至一天可以更新多次。但是如果汽车的控制系统软件出了问题，再去打补丁更新是否安全可靠？手机出现安全问题充其量就是死机，但汽车系统如果出现问题，很可能造成的就是一次交通事故，一次恶劣的社会安全事件。

赵泽良表示，随着数字化的发展，这些新技术、新应用的大规模普及背后，也面临着严峻的安全挑战，面对这些安全的课题，如何创新方法为社会和经济的发展创造更多价值，如何为数字化发展保驾护航，仍然等待着广大的网络安全从业者们不断探讨，并为之给出正确的答案。（来源：央广网）

➢ 坚持贯彻落实正确的网络安全观 筑牢新发展阶段国家网络安全屏障

习近平总书记在 2016 年 4 月 19 日网络安全和信息化工作座谈会上发表讲话（以下简称“4·19”讲话），提出要树立正确的网络安全观。此后，习总书记站在党和国家事业发展全局的高度，准确把握信息化发展大势，科学分析新形势下网络安全呈现的新特点、新趋势，在多个场合就怎样看待网络安全、如何维护网络安全提出了一系列新思想、新观念和新论断，逐步形成了以网络主权观、国家观、发展观、法治观、人民观、国际观、辩证观为主要内容的网络安全观。相关论述立意高远、思想深邃、内涵丰富，为做好新时代网络安全工作、推动网络强国建设，提供了重要指引和根本遵循。

一、正确的网络安全观指引“十三五”网络安全工作取得历史性成就

“4·19”讲话发表后，全国各地方、各部门认真贯彻落实习总书记关于“没有网络安全就没有国家安全”“网络安全为人民、网络安全靠人民”“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施”等重要论述精神，不断提升网络安全保障能力和工作水平，多措并举应对并化解网络空间风险挑战，持续推进解决关键信息基础设施防护薄弱等问题，着力维护网络安全、规范网络秩序、净化网络环境。

在习总书记“要树立正确的网络安全观”理念指导下，“十三五”期间，我国网络安全工作蹄疾步稳、硕果累累。网络安全顶层设计日趋完善，三级网信工作体系建设顺利推进，全国“一盘棋”工作格局初步形成；《网络安全法》等多部法律陆续实施，个人信息保护、数据安全等方面法律加紧制定，网络安全法治领域的“四梁八柱”基本确立；网络安全等级保护基本要求等标准相继发布，等保定级、备案、测评、监督检查等工作有序展开，关键信息基础设施安全防护能力显著提升；数据安全和个人信息保护工作扎实推进，违规收集个人

信息专项治理行动不断深化，网络空间数据安全保障体系基本形成，广大网民在网络空间的合法权益得到有效维护；网络安全学科和专业建设力度空前，网络空间安全学院在多所大学落地，政产学研结合更加紧密，网络安全人才梯队建设成效显著；《网络空间国际合作战略》《网络主权：理论与实践》《携手构建网络空间命运共同体行动倡议》等成果文件陆续发布。同时，也可以看到，网络空间国际合作日益深化、国际治网“朋友圈”持续扩大，网络空间命运共同体概念不断深入人心。

二、持续贯彻落实正确的网络安全观，准确把握新发展阶段网络安全形势

党的十九届五中全会提出，在全面建成小康社会、实现第一个百年奋斗目标之后，我国开启全面建设社会主义国家新征程、向第二个百年奋斗目标进军的新发展阶段。新发展阶段是党带领全国人民迎来从站起来、富起来到强起来历史性跨越的新阶段，也是我国从网络大国迈向网络强国的重要阶段。

正确认识党和人民事业所处的历史方位和发展阶段，是做好新发展阶段网络安全工作的重要前提。作为网络强国建设的应有之义和重要目标，在新发展阶段做好网络安全工作，需要继续认真贯彻落实习总书记关于“要树立正确的网络安全观”指示要求，深刻理解正确的网络安全观在新发展阶段的内涵外延变化，准确把握新发展阶段内外部形势变化和新技术新应用蓬勃发展带来的机遇挑战，不断强化网络安全能力建设和技术保障，更加深刻认识新发展阶段维护国家网络安全的重要转变，主动服务构建以国内大循环为主体、国内国际双循环相互促进的新发展格局。

（一）由行业安全向系统安全转变

从全球看，无论是伊朗核电站感染震网病毒、乌克兰电力设施遭遇入侵威胁，还是美国多个政府部门和私营机构遭遇太阳风（SolarWinds）攻击事件，都凸显了网络空间安全与国家安全的紧密联系。从国内看，“十四五”规划纲要提出，要在新基建、交通强国、能源革命等方面统筹推进基础设施建设，加快 5G、工业互联网、大数据中心等建设。这表明，进入新发展阶段，我国正加紧构建以信息通信设施为核心、以互联网为连接、虚拟与现实交互、网络与社会融合的互联互通数字世界。数字经济的发展使网络安全已非传统某一领域、某一系统、某一行业、某一终端的安全，互联网“连接一切”必然产生放大效应，使网络空间的安全风险外溢至经济社会发展的方方面面，任何微小的安全漏洞或安全事件都可能引发整个国计民生的“系统性灾难”。这需要在总体国家安全观的指导下，以系统思维和整体观念统筹传统安全和非传统安全，努力克服传统网络安全系统化缺失、碎片化严重、协同能力较差的问题，把维护网络安全贯穿于新发展阶段促进经济社会发展的各领域和全过程，真正做到

系统安全和总体安全。

（二）由确保数据安全向保障数字经济安全转变

党的十九届五中全会提出，加快发展数字经济，推进数字产业化和产业数字化，推动数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群。各地方政府在“十四五”规划中也提出了促进数字经济发展的系列举措，旨在激发本地区的数字经济活力。在新发展阶段，数字产业化和产业数字化发展齐头并进，将开启全面数字化和网络化的全新发展阶段，使数字经济成为新发展阶段的重要增长引擎。一方面，大量传统行业开展数字化转型，传统制造业、服务业拥抱互联网、融合互联网成为重要趋势，将促进实体经济提高生产效率、优化要素配置，为实体经济增长增添全新动力；另一方面，作为生产要素的数据本身，也将融入经济生产的链条，构成促进国民经济发展的全新生产体系。基于数据资源产权、交易流通、跨境传输、数据资源开发利用的网络安全保护需求将被集中激发，亟待建立面向保障数字经济发展与整体安全的基础制度、技术标准和保障体系。

（三）由重点领域安全到全链条安全转变

习总书记多次强调，“我们正经历百年未有之大变局”。大变局中的一个重要变量就是网络空间大国力量对比的变化。面对中国在信息通信领域技术创新、网络空间国际话语权和规则制定权的引领和崛起，以美国为首的部分西方国家在网络安全领域对我国发起前所未有的打压和攻击，从封锁华为、阻止中国信息通信领域高科技的崛起，到打压抖音、遏制中国在人工智能领域的领先优势，再到发动全球盟友组建所谓“民主技术联盟”，其主要目的在于通过对信息通信领域关键环节和重点领域的精准打压和联合围堵，切断中国实现技术赶超的供应链条和发展路径，进而实现对中国进行全面战略遏制的目的。在新发展阶段，确保关键核心供应链安全的紧迫性和必要性急剧增加，需要摈弃传统网络安全的建设思路，实施网络安全产业基础再造工程，加大重要产品和关键核心技术攻关，补齐产业链供应链短板，从而建立起以“内生安全”为基础、以关键信息基础设施为重点的全产业链安全体系。

（四）由监测处置向预警预置转变

党的十九届五中全会提出，加强经济安全风险预警、防控机制和能力建设，实现重要产业、基础设施、战略资源、重大科技等关键领域安全可控。其中，风险预警、可管可控的重点在于维护国家网络安全。随着万物互联、人机互联趋势的进一步强化，5G 等新技术在经济社会发展中所扮演的中枢角色和神经地位愈发重要，数字产业化和产业数字化步伐加快，任何苗头性、倾向性的风险都有可能引发经济社会的系统性坍塌。由此，见微知著、提前预警、风险管控，将安全风险遏制在无形、消灭在萌芽，就成为新发展阶段维护网络安全的必

然要求。正如习总书记所强调，“聪者听于无声，明者见于未形”，维护网络安全不仅要加强事中的安全检查、开展事后的应急处置，更应开展事前的预测预警；不仅要知其然，知其所以然，还要知其所未然，做到防患于未然，全方位提高预知、预警、预置能力。此外，对于已发生的风险，还要发展溯源技术、建立溯源机制，做到知道谁来了、知道是敌是友、知道它干了什么，通过准确溯源、精准定位、锁定目标产生威慑效应，让它不敢来、不敢干，切实形成全天候全方位立体化的网络安全态势感知、风险预警和精准溯源能力。

（五）由被动防御向攻防兼备转变

没有网络安全就没有国家安全。习总书记的这一重要论断在当前国际环境日趋复杂、不稳定性不确定性明显增加、世界进入动荡变革期的背景下，显得更加具有预见性和时代意义。习总书记强调，“网络安全的本质在对抗，对抗的本质在攻防两端能力的较量。”进入新发展阶段，单边主义、保护主义、霸权主义对网络空间安全构成严重威胁。时任总统特朗普在 2020 年正式承认曾授权对俄罗斯发起网络攻击，而新上任的拜登政府也在加强科技抗衡方面频频提出新政策。其他国家也在谋划成立或扩充网络战部队，开启军事备赛的线上战场。英国首相宣布已成立网络部队并向北约提供网络进攻能力，日本也成立了网络作战部队并加强与印度等国家建立合作。面对美国等西方国家咄咄逼人的网络攻击和渗透行为，传统的被动防御策略已以难以满足新形势下维护国家网络安全和经济社会发展的需要。这需要结合新发展阶段促进信息通信产业发展和保障新基建领域安全的相关需求，在强化网络安全风险预警和防御能力的同时，紧跟全球网络安全攻防技术前沿，及时掌握全球网络安全攻防技术的最新动态，千方百计在摸清对方家底情况的基础上，加强技术研发、资源调度和集中攻关，打造一批在平常时期能够形成威慑、关键时刻能够拿得出打得赢的网络安全主动防御能力，真正做到以安全对安全、以技术对技术。

三、筑牢新发展阶段国家网络安全屏障的对策建议

当前，我国网络安全环境正在发生深刻复杂的变化。进入新发展阶段，我国互联网产业和数字经济转向高质量发展，5G、人工智能、区块链、大数据等新技术加速应用，全民网络素养和安全意识得到稳步提高，做好网络安全工作的经济、技术和社会基础较为牢固。然而，也应看到，维护国家网络安全还存在核心技术受制于人、重点领域防护不强、保障体系不够健全、技术水平有待提高等问题。这需要立足我国网络安全工作实际，树立底线思维，准确识变、科学应变、主动求变，多措并举建立起维护国家网络安全的保障体系、法治体系、治理体系、技术体系和产业体系。

（一）以总体国家安全观为指导，统筹处理网络安全和经济社会发展的关系，探索建立

服务新发展格局的网络安全保障体系

坚持以总体国家安全观为指导，将保障国家网络安全放中华民族伟大复兴战略全局和世界百年未有之大变局的背景下，认真贯彻落实党的十九届五中全会提出的网络强国建设任务和发展目标，加强前瞻研究、系统谋划和顶层规划，准确把握信息化发展大势和网络安全规律动向，统筹好网络安全与总体国家安全观所包含其他领域的协同关系，正确认识网络安全在我国经济进入高质量发展阶段的基础性保障作用，研究推出一批网络安全领域的重大政策、重大举措、重大工程，以信息化发展支撑国家治理体系和治理能力现代化，以国家网络安全保障体系建设助力构建以国内大循环为主体、国内国际双循环相互促进的新发展格局。

（二）以网络空间法律法规为准绳，持续深化网络法治建设，建立以依法管网治网为核心的综合治理体系

持续深化网络法治体系建设，坚持依法管网、依法办网、依法上网，确保互联网在法治轨道上健康运行，促进网络空间与法治体系深度融合，加快推动《个人信息保护法》《数据安全法》出台。坚持围绕新发展阶段的中心任务和改革主线，依靠市场化和法治化手段，营造全社会主体依法使用网络和数据资源要素、公平参与网络竞争、平等受到法律保护的市场环境。依法加大对网络空间违法犯罪行为的打击惩处力度，不断完善网络安全领域立法、执法制度建设，及时将新兴网络技术及其风险纳入法治监管轨道。依法保护各利益主体在网络空间的合法权益，调动网络空间各主体遵法、守法的积极性和主动性，依法形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与的网络综合治理格局。

（三）以保障个人信息和重要数据安全为重点，持续开展专项治理和整治打击活动，切实维护广大网民在网络空间的根本利益

认真贯彻落实“以人民为中心”的发展思想，坚持网络安全为人民、网络安全靠人民，充分发挥广大人民维护网络安全的主体作用，整治网络生态，保护个人信息安全，持续开展网络违法违规收集使用个人信息专项治理行动，规范互联网企业和机构对个人信息的采集使用和跨境传输行为，严厉打击侵犯个人信息、电信诈骗等违法犯罪活动，切断网络犯罪利益链条，形成高压态势，让人民群众在信息化发展过程中有更多获得感、幸福感和安全感。同时，强化国家关键数据资源保护能力，完善数据产权保护制度，加大对技术专利、数字版权、数字内容产品及个人隐私等的保护力度，在关键信息基础设施行业推行数据分级分类制度，落实重点领域数据出境安全评估制度,不断增强数据安全预警和溯源能力，坚决维护广大网民在网络空间的合法权益，坚决维护国家安全与发展利益。

（四）以提高防御和威慑能力为基础，深刻洞悉网络安全技术创新和风险管控规律，打

造网络空间态势感知和风险预警技术体系

维护新发展阶段的国家网络安全，要落实习总书记“关口前移，防患未然”的重要指示精神，建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，储备一批主动防御和战略威慑力量，通过加强大数据、人工智能等技术在网络空间态势感知、风险预警和战略威慑等领域的应用转化，提高网络空间风险高预知、预警、预置能力。实现新发展阶段的自主可控，要加强网络安全关键领域技术研发和核心环节攻关，列出问题清单，明确主攻方向，在网络安全技术领域设置一批专项基金、推出一批重大项目、建设一批重大工程，广泛发动政产学研各界力量，力争突破一批基础技术、通用技术，锻造一批非对称技术、“杀手锏”技术，创造一批前沿技术、颠覆性技术，以实现网络安全领域的技术自主、安全可控。

（五）以国家网络安全产业园区为载体，构建网络安全创新发展产业生态，培育扶持一批具有国际竞争力的网络安全企业

结合新发展阶段“重要产业、基础设施、战略资源、重大科技等关键领域安全可控”和“水利、电力、供水、油气、交通、通信、网络、金融等重要基础设施安全”等保障需求，构建网络安全技术创新、基础支撑和良性发展的产业生态体系。坚持以创新驱动、协同发展、需求引领、开放合作为基本原则，在资金支持、人才引进、要素保障等领域研究制定促进网络安全产业发展的扶持政策，加大对网络安全产业的支持力度，着力突破网络安全关键技术、服务模式、产业生态、基础设施等领域的短板问题；加强创新链和产业链对接，优化网络安全产业布局，以国家网络安全产业园区建设为牵引，形成区域性龙头企业聚集效应；用好首台套、创新工程、试点示范等政策，加快培养孵化一批特色安全企业和优秀安全解决方案，提升网络安全产业供给能力，培育一批具有国际竞争力的网络安全企业，为推进新发展阶段的网络强国建设任务和“十四五”时期经济社会发展奠定产业基础。（来源：《中国信息安全》杂志 2021 年第 4 期）

➢ App“必要性”合规，需要这样依照《规定》

国家互联网信息办公室、工业和信息化部、公安部和国家市场监督管理总局（“四部委”）联合发布的《常见类型移动互联网应用程序必要个人信息范围规定》（以下简称“《规定》”）5 月 1 日正式实施。自 2021 年 3 月初《规定》颁布以来，多数企业立即针对《规定》展开自查，力争将业务所涉及的 App 类型收集的信息限制在“必要信息范围”之内，自查过程中

企业会面对怎样的难点？需要重视哪些条款？此文基于实务，讨论企业依照《规定》完成个人信息保护合规的具体路径。

一、小程序也要严格遵守《规定》

根据《规定》第二条规定，若企业运营 App 或小程序，且该 App 或小程序存在收集用户个人信息行为，则应当遵守《规定》的要求。

在实践中，小程序被纳入监管范围之内已经不存在争议，需要注意的是对小程序现有规定标准的准确把握。以微信小程序为例，不少小程序因其形式上作为小程序，相应的隐私保护设计“自行改装”。例如，大多数小程序没有实现传统 App 常见的交互，常常仅以一条主动勾选的动态链接代替需要获取用户明确同意的弹窗界。

随着《规定》的出台，小程序应对齐传统 App 的监管标准。从合规角度而言，小程序应立即调整为与传统 App 完全一致的交互设计方案。例如，需要获取用户明确同意时，小程序不应再继续简化模式，而应配置具体的符合一般要求的弹窗；又如，如果涉及调用可以收集用户个人信息敏感权限的，小程序也应当设置相应的说明窗口，在启用具体功能时获取用户的授权同意。总之，小程序并不能因为其形式上的特殊性而减免其个人信息保护的责任。

此外还应注意，小程序作为“应用软件开放平台”的接入方，本身还应遵从平台方的相应规定，向平台方报备涉及个人信息处理的举措及信息。仍以微信小程序为例，某一小程序通过平台报备而向公众公示的数据包括：开发者信息、服务和数据的来源信息（网址）、服务商信息、用户隐私及数据提示等。由于小程序的实际控制者、开发者、运营者可能并非同一主体，填报工作可能由运营者为快速上线而随意完成，导致小程序的公示信息与其实际运营信息存在差距和混淆，最终小程序的个人信息收集方（控制者）未能履行向个人信息主体

告知的义务。鉴此，在实践过程中，小程序的实际控制者应在委托其他方开发运营小程序时，在明确约定个人数据处理的数据安全责任之余，还应特别注意协同对平台的申报责任，避免侵犯个人信息主体知情权。

二、理解并明确必要个人信息的范围

《规定》出台对必要个人信息的范围进行了明确。《规定》第三条规定，“本规定所称必要个人信息，是指保障 App 基本功能服务正常运行所必需的个人信息，缺少该信息 App 即无法实现基本功能服务。具体是指消费侧用户个人信息，不包括服务供给侧用户个人信息。”据此，必要个人信息应当同时具备以下条件：

(1)是 App 基本业务功能所必需的个人信息；

(2)是消费侧用户个人信息。

这两个条件在企业实践中是高度关注的研判重点，也是《规定》对常见应用程序基本业务功能和必要个人信息进行划分的初衷。在以往的案例中，如何判断某信息是否是“App 基本业务功能所必需的个人信息”，经常是企业关注重点之一。首先，判断必要个人信息的前提是正确认定 App 的“基本业务功能”。按照《个人信息安全规范》（GB/T 35273-2020）附录 C.2 的指导，基本业务功能“应根据个人信息主体选择、使用所提供产品或服务的根本期待和最主要的需求”划定，但实践中并非每个 App 都具备清晰的设计逻辑。对于某些探索期的应用程序而言，其设计思路在于尽可能多的命中用户的潜在需求，用户可能基于功能 A 选择了该产品，也可能基于功能 B 而选择该产品，其基本功能显然会以用户的主观感受为转移，从而导致必要个人信息的范畴也存在游离。在这种情况下，基本业务功能的确认是否正确，或是否能够存在多个基本功能，成为企业个人信息保护合规判断的重要一环。

确定基本业务功能后，如何判断其“所必需的个人信息”又成为了合规工作的重点。企业需要注意，合规判断并非某单一职能部门有能力作出，比如，法务部门认为在“定位和导航软件”功能下，无需收集用户的设备信息，但是，如果产品设计方从技术角度认为必须收集设备信息确保运营环境安全，则法务和技术部门需要共同根据《规定》做出统一判断。

三、切实落实对个人信息主体的告知义务

如上所述，必要个人信息作为用户所选择的基本业务功能所必需的个人信息，可以视为符合《个人信息安全规范》规定的“履约必要”条件，从而豁免个人信息控制者获取个人信息主体授权同意的义务，符合《规定》要求的必要个人信息无需征得个人信息主体的授权同意。但是个人信息控制者仍应落实对个人信息主体的告知义务。因此，《隐私政策》中仍应对基于“履约必要”条件收集的个人信息向个人信息主体进行告知。

同时，如果基于“履约必要”条件收集的个人信息将用于数据分析并最终用于实现自动化决策、个性化推荐场景时，其目的显然已经超越了履约目的，因此应获取个人信息主体的额外授权同意。出于产品合规的目的，这个授权同意应当在告知个人信息主体必要个人信息范围时一并告知并获得授权同意。同时，针对因授权同意而获取的个人信息，即便“履约必要”作为合法处理理由之一，仍应赋予其撤销权，且为保障该撤销权不影响基本功能的实现，基于“履约必要”目的和基于数据分析目的而收集的数据应分开表单存储。诸如此类，隐私设计细节，均应在产品设计之初考虑，并落实在《隐私政策》中告知用户。

四、对标《规定》，“升级”对个人信息和个人敏感信息的表述

《规定》第五条对于 39 类常见类型 App 的基本功能和必要个人信息范围以列举形式进行了明示，供企业在设计、投产、复核其自身 App 的合规情况作为有效对照。

需要注意的是，《规定》对不同类别 App 个人信息获取范围做了明确，相对以往的规范有了增减，新增表述字段梳理如下：

APP 类型　　新增必要个人信息字段

网上购物类　支付渠道

餐饮外卖类　支付渠道

交通票务类　车次/船次/航班号、席别/舱位等级、座位号（如有）

房屋租售类　面积/户型、期望售价或租金

问诊挂号类　预约挂号的医院和科室

旅游服务类　旅游目的地、旅游时间

酒店服务类　入住和退房时间、入住酒店名称

演出票务类　观演场次、座位号（如有）；支付渠道

这些被明确认定为个人信息的表述，几乎都是个人信息中能够反映个人信息主体行踪轨迹、健康状况和财产状况的个人信息，如果按照“一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等”的标准判断，此类信息均足以视为个人敏感信息。

鉴此，企业在个人信息保护合规工作中，需要业务进一步“升级”：

（1）在合规表述中，扩充个人信息和个人敏感信息的字段示例范围；

（2）扩充数据分级分类标准，将能够反映个人信息主体行踪轨迹、健康状况和财产状况的个人信息提高敏感级别。（来源：中国网络空间安全协会）

四、政府之声

➢ 工信部深入推进“断卡行动”四大举措重拳出击电信网络诈骗

2021 年 5 月 12 日，工业和信息化部在北京召开信息通信行业防范治理电信网络诈骗工作电视电话会议，传达学习习近平总书记关于打击治理电信网络新型违法犯罪重要指示精神和李克强总理批示要求，落实国务院打击治理电信网络新型违法犯罪工作部际联席会议工作部署，对信息通信行业深入推进防范治理电信网络诈骗工作进行了再动员、再部署。工业和信息化部党组成员、副部长刘烈宏，部总工程师韩夏，国务院联席办主任、公安部刑事侦查局局长刘忠义出席会议。

会议指出，工业和信息化部始终高度重视防范治理电信网络诈骗工作，多措并举持续整治重点业务和突出问题，积极推进技术手段建设，支撑配合公安机关严打电信网络诈骗犯罪，取得阶段性成效。2020 年以来，信息通信行业充分发挥技术手段作用，持续加大电话卡治理力度，累计拦截涉诈电话 7.3 亿次、短信 15.5 亿条，处置涉诈号码 1865 万余个，为公安机关提供线索近 100 万条，协助劝阻受害用户 293 万人，有力维护了人民群众的财产安全。

会议强调，面对电信网络诈骗犯罪新特点和复杂形势，全行业要坚决贯彻落实习近平总书记重要指示精神，深刻认识当前电信网络诈骗犯罪形势的严峻性和复杂性，将防范治理工作作为全行业的重要政治任务，进一步增强工作责任感和紧迫感，支撑配合公安机关深入推

进防范治理工作，切实维护人民群众财产安全和合法权益。

会议对信息通信行业防范治理电信网络诈骗工作进行了全面部署，强调要突出源头治理与综合治理，全面构建行业反诈工作体系。一是健全部省两级行业主管部门与公安机关协作配合机制，完善部、省、企协同的行业联动工作机制，形成统一联动、责任明晰、机制畅通、运转高效的工作体系，二是坚持技管结合、以技管网，统筹调度全行业反诈技术资源，提升部省两级反诈平台能力，强化重点业务技术监管能力建设，构建起全国一体化的技术防控体系。三是严肃落实责任，强化电话卡、物联网卡等重点业务风险整治，下大力气解决一批重点难点问题，坚决从根源上堵住行业问题漏洞。四是进一步提升大数据涉诈线索分析能力，压紧压实电信和互联网企业安全管理责任，巩固深化反诈长效治理机制。

针对当前行业治理中最为紧迫的电话卡、物联网卡管理问题，会议要求在前期工作基础上，进一步聚焦突出问题，以更为严格的精准治理措施，更加深入地推进“断卡行动”：一是建立完善“二次实人认证”、快速停复机协同工作机制；二是强化异常卡监测发现，着力清理整顿“睡眠卡”、“静默卡”、“一证多卡”、虚拟运营商存量卡等高风险号卡；三是加大对涉诈互联网账号及网上涉诈信息的关联处置力度；四是通过强化绩效考核、优化调整考核指标、建立挂牌整治制度等方式进一步夯实企业反诈责任体系。（来源：工信部网络安全管理局）

➢ 国家网信办发布《汽车数据安全管理若干规定》征求意见

2021 年 5 月 12 日，为加强个人信息和重要数据保护，规范汽车数据处理活动，根据《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同有关部门起草了《汽车数据安全管理若干规定（征求意见稿）》，现向社会公开征求意见。

国家互联网信息办公室发布关于《汽车数据安全管理若干规定（征求意见稿）》公开征求意见的通知。其中包含“运营者收集个人信息应当取得被收集人同意，法律法规规定不需取得个人同意的除外”；“个人信息或者重要数据应当依法在境内存储，确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估”等内容。（来源：中国网信网）

- **汽车数据安全管理若干规定（征求意见稿）**
- **全文：**http://www.cac.gov.cn/2021-05/12/c_1622400511898266.htm

➢ 《广东省社会信用条例》6 月 1 日生效，禁止商家采集个人生物识别信息

2021 年 5 月 17 日，《广东省社会信用条例》将自 2021 年 6 月 1 日起施行。广东省人大常委会召开新闻发布会，介绍《条例》有关情况。

省人大法制委副主任委员黄伟忠介绍，《条例》强化信息安全管理，特别强调对个人信息安全的保护，在相关环节设置了一系列保障措施。如第二十二条规定，采集市场信用信息，禁止采集自然人的宗教信仰、血型信息，疾病、病史信息，基因、指纹等生物识别信息以及法律、行政法规规定禁止采集的其他信息。

《条例》还明确了相应的法律责任，规定信用服务机构、信用服务行业组织、其他企事业单位、社会组织及其工作人员违反条例规定，采集禁止采集的个人信息的，由县级以上人民政府社会信用主管部门或者法律、法规规定的部门责令改正，对单位处五万元以上五十万元以下的罚款;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下的罚款;

有违法所得的，没收违法所得。为完善失信约束制度，对失信惩戒措施清单，规定应当执行全国失信惩戒措施基础清单，省、地级以上市确因社会治理、市场监管和公共服务的需要，只能依据地方性法规，才可以制定适用于本地的失信惩戒措施补充清单。《条例》对补充清单的内容、程序均作了规范，并要求公开征求意见，由本级人民政府同意并按规定备案。严格限制补充清单的范围为：约谈、重点监管、降低等次、撤销相关荣誉等 8 类措施，禁止在失信惩戒措施清单外违法违规实施惩戒措施。（来源：广东人大网）

- **广东省社会信用条例**
- **全文：**http://www.rd.gd.cn/zxfb/202103/t20210325_183314.html

➢ CNCERT 发布《2020 年我国互联网网络安全态势综述》报告

2021 年 5 月 26 日，国家互联网应急中心（CNCERT）编写的《2020 年我国互联网网络安全态势综述》报告（以下简称“2020 年态势报告”）正式发布。为全面反映我国网络安全的整体态势，CNCERT 自 2010 年以来，每年发布前一年度网络安全态势情况综述，至今已连续发布 12 年，对我国党政机关、行业企业及社会了解我国网络安全形势，提高网络安全意识，做好网络安全工作提供了有力参考。

2020 年，全球突发新冠肺炎疫情，抗击疫情成为各国紧迫任务。不论是在疫情防控相

关工作领域，还是在远程办公、教育、医疗及智能化生产等生产生活领域，大量新型互联网产品和服务应运而生，在助力疫情防控的同时也进一步推进社会数字化转型。与此同时，安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁日益凸显，有组织、有目的的网络攻击形势愈加明显，为网络安全防护工作带来更多挑战。

2020 年态势报告以 CNCERT 宏观网络安全监测数据与工作实践为基础，综合各类安全威胁、事件信息，网络安全事件应急处置以及网络安全威胁治理实践等内容。报告主要分为三个部分：

一是总结 2020 年我国互联网网络安全状况。报告总结了我国在网络安全法律法规建设完善、网络威胁治理等所取得的重要成果。重点从 APT 攻击、数据安全、安全漏洞、恶意程序、网络反诈、工业控制系统安全等六个方面对全年突出的网络安全状况特点进行了梳理。

二是预测 2021 年网络安全热点。报告提出六点预测，认为 APT 攻击威胁、个人信息保护、供应链安全、关键信息基础设施安全、远程协作安全风险、大数据安全等将成为 2021 年网络安全领域值得关注的热点。

三是梳理网络安全监测数据。报告从攻击来源、攻击对象、攻击规模等维度，通过丰富的宏观安全监测数据统计分析，对恶意程序、安全漏洞、拒绝服务攻击、网站安全、云平台安全、工业控制系统安全、区块链安全等七个方面进行了梳理。（来源：国家互联网应急中心）

- **《2020 年我国互联网网络安全态势综述》全文：**
- https://www.cert.org.cn/publish/main/upload/File/2020%20CNCERT%20Cybersecurity%20Analysis.pdf

五、本期重要漏洞实例

➢ Microsoft 发布 2021 年 5 月安全更新

发布日期：2021-05-18
更新日期：2021-05-18
描述：
5 月 11 日，微软发布了 2021 年 5 月份的月度例行安全公告，修复了其多款产品存在的 55 个安全漏洞。受影响的产品包括：Windows 10 20H2 & Windows Server v20H2（24 个）、Windows 10 2004 & Windows Server v2004（24 个）、Windows 10 1909 & Windows Server v1909（16 个）、Windows 8.1 & Server 2012 R2（12 个）、Windows Server 2012（11 个）、Windows RT 8.1（11 个）和 Microsoft Office-related software（11 个）。利用上述漏洞，攻击者可进行欺骗，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-2021-31166	**HTTP 协议栈远程代码执行漏洞**	严重 远程代码执行	Windows 10 Server, version 2004 Server, version 20H2
CVE-2021-28476	**Hyper-V 远程代码执行漏洞**	严重 远程代码执行	Server, version 20H2 Server, version 2004 Server, version 1909 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-31194	**OLE Automation 远程代码执行漏洞**	严重 远程代码执行	Server, version 20H2 Server, version 2004 Server, version 1909 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-26419	**Scripting Engine 内存破坏漏洞**	严重 远程代码执行	Internet Explorer 11
CVE-2021-26422	**Skype for Business 和 Lync 远程代码执行漏洞**	重要 远程代码执行	Skype for Business Server 2015 CU11 Skype for Business Server 2019 CU5

			Lync Server 2013 CU10
CVE-2021-28455	**Microsoft Jet Red Database Engine 和 Access Connectivity Engine 远程代码执行漏洞**	重要 远程代码执行	Windows Server 2012 R2 Windows Server 2012 Windows RT 8.1 Windows Server 2016 Windows 10 Server, version 20H2 Server, version 2004 Server, version 1909 Windows Server 2019 Office 2013/2016/2019 365 Apps for Enterprise
CVE-2021-28474	**Microsoft SharePoint Server 远程代码执行漏洞**	重要 远程代码执行	SharePoint Foundation 2013 SharePoint Server 2019 SharePoint Enterprise Server 2016
CVE-2021-31175	**Microsoft Office 远程代码执行漏洞**	重要 远程代码执行	Excel 2013 Office 2016 Office Web Apps Server 2013 Office 2013 Office Online Server Office 2019 Excel 2016 365 Apps Enterprise
CVE-2021-31180	**Microsoft Office Graphics 远程代码执行漏洞**	重要 远程代码执行	Office 2013 Word 2013 Word 2016 Office 2019 365 Apps Enterprise

来源：https://msrc.microsoft.com/update-guide/releaseNote/2021-May

➢ 关于 VMware vCenter Server 存在远程代码执行漏洞的安全公告

发布日期：2021-05-26
更新日期：2021-05-26
受影响系统：
VMware vCenter Server 7.0V
Mware vCenter Server 6.7V
Mware vCenter Server 5.5
Cloud Foundation (vCenter Server) 4.x
Cloud Foundation (vCenter Server) 3.x
描述：

CVE(CAN) ID: CNTA-2021-0020

2021 年 5 月 26 日，国家信息安全漏洞共享平台（CNVD）收录了 VMware vCenter Server 远程代码执行漏洞（CNVD-2021-37150，对应 CVE-2021-21985）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞相关细节尚未公开，VMware 公司已发布新版本修复漏洞，建议用户尽快更新至最新版本。VMware vSphere 是美国威睿公司推出一套服务器虚拟化解决方案，包括虚拟化、管理和界面层。VMware vSphere 的两个核心组件是 ESXi 服务器和 vCenter。VMware ESXi 是 VMware 的裸机虚拟机管理程序，用以创建运行虚拟机和虚拟设备。VMware vCenter Server 是管理整个 VMware 虚拟化基础架构的软件，用于集中管理多个 ESXi 主机和以及在 ESXi 主机上运行的虚拟机。用户可以通过 vSphere Client 登录到 vCenter Server 来管理 vSphere 清单，使用 vSphere Client 需要 Web 浏览器支持。

2021 年 5 月 25 日，VMware 公司发布多个关于 vCenter Server 的安全公告，其中包括 VMware vCenter Server 存在远程代码执行漏洞（CNVD-2021-37150，对应 CVE-2021-21985）。该漏洞存在于 vSphere Client（HTML5）包含的运行状况检查插件 vSAN（Virtual San Health Check）中，该插件在 vCenter Server 中默认启用。由于缺乏必要的输入验证，攻击者可以向开放 443 端口的 vCenter Server 服务器发送恶意构造的请求，在目标系统上执行任意代码，获得目标服务器的权限，实现对 vCenter Server 的远程代码执行。CNVD 对上述漏洞的综合评级为“高危”。

建议：

厂商补丁：

VMware

目前，VMware 公司已发布新版本修复上述漏洞，CNVD 建议用户立即升级至最新版本：

https://www.vmware.com/security/advisories/VMSA-2021-0010.html

附：参考链接：

https://www.vmware.com/security/advisories/VMSA-2021-0010.html

➢ Google Chrome ANGLE 堆缓冲区溢出漏洞

发布日期：2021-05-18

更新日期：2021-05-18

受影响系统：

Google Chrome <90.0.4430.93

描述：

CVE(CAN) ID: CVE-2021-21233

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。

Google Chrome 90.0.4430.93 之前版本中的 ANGLE 存在堆缓冲区溢出漏洞。远程攻击者可利用漏洞通过特制的 HTML 页面利用堆损坏进行潜在攻击。

建议：

厂商补丁：

Google

厂商已发布了漏洞修复程序，请及时关注更新：

https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html

➢ IBM WebSphere Application Server XML 外部实体注入漏洞

发布日期：2021-05-25
更新日期：2021-05-28
受影响系统：
IBM Websphere Application Server 9.0
IBM Websphere Application Server 8.5
IBM Websphere Application Server 8.0
IBM WebSphere Application Server Liberty 17.0.0.3<= Version <=21.0.0.5
描述：

CVE(CAN) ID: CVE-2021-20492
IBM WebSphere Application Server（WAS）是美国 IBM 公司的一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。
IBM WebSphere Application Server 8.0、8.5、9.0 和 Liberty Java Batch 存在 XML 外部实体注入漏洞。远程攻击者可利用该漏洞泄露敏感信息或消耗内存资源。
<*来源：Kylinking（NSFOCUS Security Team）
链接：https://www.ibm.com/support/pages/node/6456017
*>
建议：

厂商补丁：
IBM

IBM 已经为此发布了一个安全公告（6456017）以及相应补丁:
6456017：Security Bulletin: WebSphere Application Server Java Batch is vulnerable to an XML External Entity Injection (XXE) vulnerability (CVE-2021-20492)
链接：https://www.ibm.com/support/pages/node/6456017

六、本期网络安全事件

➢ 美国最大燃油管道运营商 Colonial Pipeline 遭勒索软件攻击

2021 年 5 月 11 日，当地时间 5 月 9 日，美国联邦政府交通部联邦汽车运输安全管理局宣布美国 17 个州和华盛顿特区进入紧急状态，以应对勒索软件的攻击，该攻击迫使美国最大的成品油管道运营商 Colonial Pipeline 关闭了一条关键的运输管道，此管道承担美国东岸 45%的燃料供给。

据 BBC、路透社等外媒消息多方信源确认称，这起勒索软件袭击是一个名为“暗面”（DarkSide）的网络犯罪组织所为。而这个组织不但研发软件、培训“下线”，坐收提成，直接把勒索袭击当一门生意运营了起来，甚至还广而告之，发起新闻稿，邀请记者采访。

“暗面”勒索袭击手法曝光远程办公或给黑客留下可乘之机

据 BBC 消息，“暗面”在 5 月 6 日就侵入了 Colonial Pipeline 的网络，将近 100GB 的数据作为要挟筹码；在获取这些数据后，还锁住了一些电脑和服务器上的数据，并在 7 日索要赎金。“暗面”威胁称，若不如期支付，就将把这些数据泄露到网上。知情人士表示，其索要的赎金是价值或高达数百万美元的虚拟货币。

据悉，“暗面”在完成袭击后，受害者除了能看到电脑屏幕上出现的勒索通知，还会收到一个信息包。“暗面”会通知受害者称“电脑和服务器已经被加密了”，还会列出盗取的数据类型清单，并发出一个“个人泄露页面”链接。这个页面已经完成了数据加载。如果企业

或组织没有在截止时间前付款，该页面就会自动公布数据。“暗面”还会告知受害者，将会提供其已经获取的数据的证据，并准备从受害者的网络上将其删除。

这起勒索袭击事件表明，关键性的国家工业基础设施在网络犯罪时代面临着越来越高的勒索风险。专家分析认为，Colonial Pipeline 遭袭还是因为新冠疫情——疫情期间，很多工程师都在家远程工作，经常远程访问公司的控制系统，由此给了黑客可乘之机。

伦敦一家追踪全球网络犯罪组织的网络安全公司“数码阴影”（Digital Shadows）联合创始人詹姆斯 •坎贝尔认为，“暗面”是购买了如 TeamViewer 和微软远程桌面（Microsoft Remote Desktop）之类的远程连接控制软件的账户登录信息。

卖软件训练“下线”坐收提成设有媒体中心和受害者热线

据“数码阴影”介绍，“暗面”不是一个单纯进行勒索袭击的黑客组织，而是做着一门勒索袭击的生意——卖软件，训练下线，坐收提成。据悉，“暗面”开发出用来加密和盗取数据的软件，再训练“分支、下线”。这些下线会拿到一个设计完整的工具箱，其中包括用于袭击的软件、索要赎金的邮件模板，以及如何执行袭击的相关培训。而这些“下线”、网络犯罪分子每一次成功勒索攻击，就会向该组织支付一定比例的收益。据路透社消息，“暗面”是越来越专业化的勒索组织之一。该组织有媒体中心，承诺“24 小时快速回复”，还有受害者热线，甚至还有行为准则，将自己打造成“值得信赖的”商业合作伙伴。

波士顿的网络安全公司“赛博瑞森”（Cybereason）CEO 利奥尔 • 迪夫指出，去年，这个组织横空出世，很快就来了一大波犯罪。仅他的客户中就有 10 多个在短短几个月内遭到该组织攻击。因此，他认为这应该是个由一些黑客老手组成的组织。据 BBC 消息，今年 3 月，“暗面”发布了一款“比以前更快加密数据”的新软件，还发布了一份新闻稿，邀请记者前去采访报道。该组织还在暗网上架设有一个网站，详细地吹嘘自己的“事迹”——列出其攻击过的所有公司、具体曾盗得了什么等，其发布的相关名单中包括美国和欧洲的 80 多家企业。此外，该网站甚至还有一个“职业道德”页面，列出了一些不会攻击的组织名单。

詹姆斯 • 坎贝尔补充道，其公司的研究显示，从“暗面”的攻击行为看来，其似乎在避免攻击独联体（CIS）国家的企业。

一次“失算”的袭击？惊动美国政府与 FBI 后一改高调

据 BBC 消息，美国 Colonial Pipeline 公司称，袭击发生后，该公司一直在同执法部门、网络安全专家以及能源部合作，努力恢复服务。截至当地时间 9 日晚，其 4 条主要管道依然处于下线状态，只有一些终端和交付点之间的部分小型支线管道已经恢复运行。

受此次事件影响，周一亚市早盘，美国汽油期货一度上涨 4.2%至每加仑 2.217 美元，为

2018 年 5 月以来最高。此外，美国取暖油期货也跳升至 2020 年 1 月以来的高点。国际油价方面，美国 WTI 原油期货价格上涨 1.08%至 65.59 美元/桶，布伦特原油期货上涨 1.1%至 69.03 美元/桶。有石油分析师表示，这次袭击对燃料供应和价格的影响取决于输油管道的关闭时间。一两天的停运影响是最小的，但停运五六天可能会导致石油短缺和价格上涨。长时间延误将对亚特兰大和北卡罗来纳州夏洛特的机场燃料造成重大影响。（来源：红星新闻）

➢ 细思极恐！你家电视有可能正在扫描家庭所有联网设备

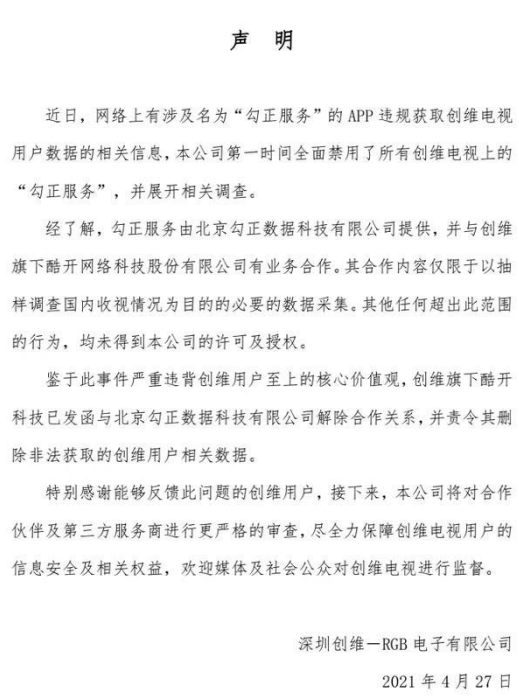
2021 年 5 月 9 日，近日有网友反映，在使用创维电视时，发现电视每 10 分钟就扫描一遍所有的联网设备，用户的主机名、MAC 地址和 IP 地址甚至周边邻居的 wifi 名称等隐私信息都被打包发送到了一家名为“勾正数据”的企业。这家勾正数据，为何能进入创维电视内置的应用程序？拿到的数据又被用作什么？

超限收集用户信息隐私安全如何保护？

资料显示，勾正数据是一家智能营销第三方大数据公司。勾正拿到的数据，大多用来做开机广告和贴片广告的优化。该公司的服务涵盖了大量视频门户网站与电视厂商。其数据覆盖了 1.03 亿的智能电视终端，占全网设备量的 55%。

事后，**创维公司发布声明称**，勾正公司与创维旗下的酷开公司有业务合作，但合作内容仅限于以抽样调查国内收视情况为目的的必要数据采集。其他任何超出此范围的行为，均未得到许可及授权。目前已经解除合作关系，并责令其删除非法获取的创维用户相关数据。

数码评论员黄浩称，提取用户画像卖钱，已经成为很多数据公司的主要业务，广告商甚至不少视频平台都需要他们提供数据，电视机开屏广告、视频 APP 的推送，能做到不同用户看到不同内容，都是根据用户画像来进行的定义，但勾正如此频繁、深入的用户画像收集，已经超过了本该有的限度。



声　明

近日，网络上有涉及名为“勾正服务”的 APP 违规获取创维电视用户数据的相关信息，本公司第一时间全面禁用了所有创维电视上的“勾正服务”，并展开相关调查。

经了解，勾正服务由北京勾正数据科技有限公司提供，并与创维旗下酷开网络科技股份有限公司有业务合作。其合作内容仅限于以抽样调查国内收视情况为目的的必要的数据采集。其他任何超出此范围的行为，均未得到本公司的许可及授权。

鉴于此事件严重违背创维用户至上的核心价值观，创维旗下酷开科技已发函与北京勾正数据科技有限公司解除合作关系，并责令其删除非法获取的创维用户相关数据。

特别感谢能够反馈此问题的创维用户，接下来，本公司将对合作伙伴及第三方服务商进行更严格的审查，尽全力保障创维电视用户的信息安全及相关权益，欢迎媒体及社会公众对创维电视进行监督。

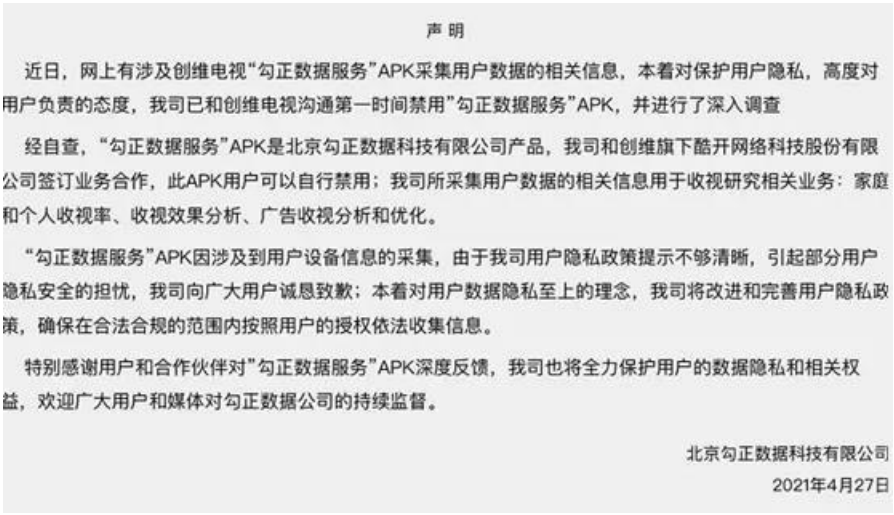
深圳创维－RGB 电子有限公司

2021 年 4 月 27 日

数码评论员黄浩：其实每个人看到的电视机推送的内容是不一样的，电视机厂商或者是数据服务商，通过后台在收集用户的数据。工信部有明文规定，可以收集用户数据，因为如果消费者想享受这种自动推送，肯定要给予这些智能设备一定的权限，但是有一个度。

为了制定用户画像，真的还要做到扫描家中互联网连接设备甚至周边 wifi 信息吗？黄浩解释，通过扫描不同的设备，数据服务商能够对用户进行更精准的分析。

事后，**勾正公司也回应称**，该公司所采集用户数据的相关信息用于收视研究相关业务：家庭和个人收视率、收视效果分析、广告收视分析和优化。“勾正数据服务”因涉及到用户设备信息的采集，由于用户隐私政策提示不够清晰，引起部分用户隐私安全的担忧，向广大用户诚恳致歉；本着对用户数据隐私至上的理念，公司将改进和完善用户隐私政策，确保在合法合规的范围内按照用户的授权依法收集信息。



声明

近日，网上有涉及创维电视“勾正数据服务”APK采集用户数据的相关信息，本着对保护用户隐私，高度对用户负责的态度，我司已和创维电视沟通第一时间禁用”勾正数据服务”APK，并进行了深入调查

经自查，“勾正数据服务”APK是北京勾正数据科技有限公司产品，我司和创维旗下酷开网络科技股份有限公司签订业务合作，此APK用户可以自行禁用；我司所采集用户数据的相关信息用于收视研究相关业务：家庭和个人收视率、收视效果分析、广告收视分析和优化。

“勾正数据服务”APK因涉及到用户设备信息的采集，由于我司用户隐私政策提示不够清晰，引起部分用户隐私安全的担忧，我司向广大用户诚恳致歉；本着对用户数据隐私至上的理念，我司将改进和完善用户隐私政策，确保在合法合规的范围内按照用户的授权依法收集信息。

特别感谢用户和合作伙伴对”勾正数据服务”APK深度反馈，我司也将全力保护用户的数据隐私和相关权益，欢迎广大用户和媒体对勾正数据公司的持续监督。

北京勾正数据科技有限公司

2021年4月27日

对此，黄浩认为，如此解释难以让人信服，因为消费者对于收集了哪些信息并不知情：

数码评论员黄浩：收集信息要有度，扫描家里路由器全网连接的所有内容已经过度了。在收集数据的时候是要给予消费者明确的公示跟告知，让消费者来做数据收集的决策者，而不能说在消费者不知情的情况下就把数据收集了。

大数据收集难以举证用户如何维权？那么这种行为是否涉嫌违法？

北京岳成律师事务所律师岳岫山介绍，我国《民法典》、《网络安全法》和《消费者权益保护法》中，对于个人信息的收集有明确的要求，既遵循合法、正当、必要性原则，商家取得信息前，必须要经过用户同意。

北京岳成律师事务所律师岳岫山：商家在取得这些信息之前，必须是要经过用户的同意才可以，要有明确的授权，而且这些授权不应该是捆绑取得。很多商家明知法律有这样的要求，但却故意掠夺用户的信息，因为这些信息能给他们带来相应的收益，按照法律的规定，这种侵权应当停止侵害，赔偿损失，之前违法获取信息的行为，或者说所获取的信息，应当进行清理和删除。岳岫山也承认，在司法实践中，由于大数据收集有一定专业性，用户很难证明损失，更别提对商家提起诉讼，这就更需要相关行业主管部门主动出击。

北京岳成律师事务所律师岳岫山：在实际的司法实践过程当中，用户很难证明自己有什么样的损失，这也是导致很多商家肆无忌惮的使用这种侵权手段获取信息的原因之一。对他们来讲，是没有违法成本或者说侵权成本的，这其实也需要相关主管部门，不管是市场监管部门还是网络主管部门，对这类行为要及时的进行清理，对相应的行为进行处罚和处理，形成有效的威慑。

超限收集用户信息，不光没有用户明确的授权，绝大多数人甚至无法察觉，收集的信息又真的如数据公司所说用于收视率分析、广告优化等吗？大数据作为新兴事物，又有多少人能像专业人员一样留存证据？看电视本是工作和生活的调剂品，却还要和电视厂商、数据服务商勾心斗角，匹夫无罪，怀璧其罪，电视厂商、数据服务商关心的恐怕不仅是用户的家里网速多少，每天看什么样的节目，更多的还是据此分析来推送广告获取利益，这里面又是否涉及用户数据买卖我们不得而知。少点套路，多点真诚，莫让智能电视成为直播用户生活的工具。（来源：央广网）

➢ 爱尔兰遭遇最严重的网络攻击 黑客试图加密国家卫生数据并勒索金钱

2021 年 5 月 14 日，爱尔兰一位部长表示，对爱尔兰卫生服务计算机系统的网络攻击，可能是爱尔兰遭遇的最严重的网络犯罪攻击，这次攻击直指爱尔兰国家卫生系统的核心。

攻击发生后，卫生服务部门已经暂时关闭了其 IT 系统以进行保护。担任公共采购和电子政务部长的 Smyth 先生说这是一次国际攻击，这些是网络犯罪团伙，在寻找金钱。他们试

图对爱尔兰国家卫生数据进行加密和锁定。然后试图向爱尔兰当局勒索金钱以赎回数据。爱尔兰卫生服务执行局表示，它已经关闭系统，采取预防措施，以进一步保护它们并评估情况。

国家网络安全中心（NCSC）表示：爱尔兰卫生服务执行局在周五凌晨意识到它的一些系统受到了重大的勒索软件攻击，NCSC 被告知这个问题并立即启动了危机应对计划。爱尔兰卫生部长斯蒂芬-唐纳利说，这一事件正在对卫生和社会护理服务产生严重影响。

如果这种情况持续到周一，爱尔兰我卫生系统将处于非常严重的状况，将取消许多服务。爱尔兰一些医院正在报告服务中断。都柏林的 Rotunda 医院由于严重紧急情况已经取消了门诊。都柏林的国家妇产医院也说，由于一个重大的 IT 问题，其服务在周五会有重大干扰。

都柏林的 St Columcille 医院说，一些虚拟预约和与电子记录有关的事项被推迟了。克鲁姆林医院的爱尔兰儿童健康组织（CHI）通知人们，出现了延误，所有的虚拟/在线预约都被取消。由中西部六家医院组成的 UL 医院集团在一份声明中说，参加其服务的病人预计会有长时间延误，但是急诊服务仍在运作。

但是爱尔兰全国 Covid-19 疫苗接种和测试将正常进行。早些时候，爱尔兰卫生服务执行局首席执行官 Paul Reid 告诉 RTÉ 的《爱尔兰之晨》，它正在努力控制对其 IT 系统的勒索软件攻击。他说，网络攻击正在影响涉及所有核心服务。攻击的重点是访问存储在中央服务器上的数据。他说这是一个重大事件，但现阶段黑客还没有提出赎金要求。（来源：cnBeta）

➢ 印度航空 450 万客户数据遭黑客窃取

2021 年 5 月 22 日，据外媒 TechCrunch 报道，当地时间 22 日，印度航空官网发布消息称，该公司大约 450 万名客户的数据遭黑客窃取，黑客窃取的数据包括乘客的姓名、信用卡信息、出生日期、联系信息、护照信息、机票信息。

印度航空在声明中表示，在乘客服务系统（PSS）被黑客攻击两个月后公司才确认的这次泄漏的具体信息。这次攻击使公司损失了过去十年（2011 年 8 月 26 日至 2021 年 2 月 3 日）在印度航空公司注册的乘客的数据。不过值得一提的是，虽然客户的姓名、信用卡、护照等信息被窃取了，但是其 CVV/CVC（一种信用卡校验码）数据却并没有泄漏，因为公司敦促乘客“在适用的情况下”更改密码，以确保其个人数据的安全。

印度航空公司还表示，公司目前已采取措施确保数据安全，包括调查数据安全事件、保护被破坏的服务器、聘请外部数据安全事件专家、通知信用卡发卡机构并与之联络，以及重新设置印度航空公司 FFP 项目的密码。

据悉，印度航空公司并不是此次黑客网络攻击事件的唯一受害者，另外几家航空公司也受到了影响，包括新西兰航空、国泰航空、芬兰航空、济州航空、汉莎航空、马来西亚航空和新加坡航空公司客户的数据都遭到了黑客不同程度的窃取。（来源：TechCrunch）

➢ 男子用木马软件远程“捕获”消费者信息获刑

2021 年 5 月 25 日，为找到定向客户，张某翔通过电脑木马软件远程获取其他公司消费者信息后，向消费者售卖产品获取利润。近日，经广灵县法院审理查明，张某翔非法获取 315 条消费者消息，已构成侵犯公民个人信息罪，判处有期徒刑 1 年，缓刑 1 年，并处罚金 5000 元。

经审理查明，自 2018 年 11 月开始，张某翔雇佣蔡某、郭某、段某，在广灵县壶泉镇秀水二期其租住房内销售男性补品本草膏方。张某翔从网友处购买远程控制软件，并上网搜索同行公司，以客户名义与对方公司销售员聊天，聊天中张某翔向对方发送带有木马程序的文档，郭某和蔡某远程监控被植入木马程序的电脑，在监控对方与其客户聊天内容中，获取客户个人信息后截图并上报张某翔，张某翔安排段某向客户电话推销其产品，交易达成后，张某翔将其从网上购买的本草膏方通过快递发货，货到付款，张某翔再通过快递账户提现。截至 2020 年 1 月，张某翔共获取客户个人信息 315 条，销售本草膏方 33.2679 万元，获利 20 余万元。

法院认为，张某翔违反国家有关规定，通过给他人电脑植入木马程序，远程监控对方与客户聊天内容，非法获取公民个人信息 315 条，情节严重，其行为侵犯了公民个人身份信息的安全和公民身份管理秩序，触犯了《中华人民共和国刑法》的规定，构成侵犯公民个人信息罪，公诉机关指控事实存在，罪名成立。张某翔到案后自愿如实供述自己的罪行，系坦白，依法可从轻处罚。被告人当庭自愿认罪认罚，认罪态度较好，可酌情从轻处罚。故法院决定

对其从轻处罚，并依法适用缓刑。对辩护人的辩护意见予以采纳。综上，依据《中华人民共和国刑法》《最高人民法院、最高人民检察院〈关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释〉》的规定，判处张某翔犯侵犯公民个人信息罪，判处有期徒刑 1 年，缓刑 1 年，并处罚金 5000 元。

法官说法：侵犯公民个人信息罪认定方式之一是：窃取或者以其他方法非法获取公民个人信息的行为。对此，需要着重把握“其他方法”的范围问题。“窃取”是指采用秘密的或不为人知的方法取得他人个人信息的行为。“其他方法”，是指“窃取”以外的其他方法，如通过收买、欺骗等方法非法获取公民个人信息。实际上，窃取也是非法获取的方式之一。关于“其他方法”是否必须自身具有非法的性质，即其他方法是否只包括诈骗、胁迫等自身具有非法性质的方法，而不包括购买、接受赠与等自身不具有非法性质的方法，存在不同认识。从行为人获取行为的本质属性角度加以判断，而不论获取行为是否违反法律的禁止性规定，即只要行为人没有获取公民个人信息的法律依据或者资格而获取相关个人信息的，即可以认定系“非法获取”。（来源：山西法制报）

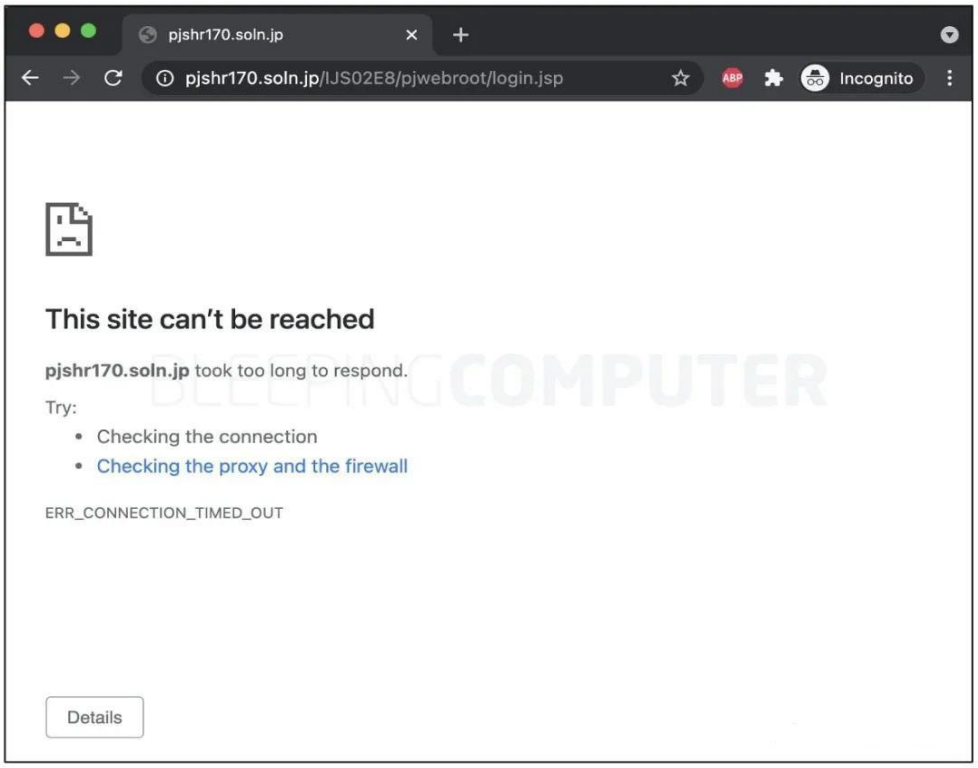
➢ 供应商被黑客攻击 日本政府大量敏感数据泄露

2021 年 5 月 28 日，日本国土交通省及国家网络安全中心（NISC）宣布，攻击者未授权访问了富士通 ProjectWEB 工具，并借此窃取到部分政府客户数据。

ProjectWEB 是一个完整的 SaaS（软件即服务）解决方案，可提供项目管理、安全检查工具、质量保证、修订管理和进度监视工具，主要供企业及各类组织的项目经理与利益相关方高效交换信息。该软件已被日本各政府机构和几家主要的私人公司广泛使用。 至少 76000 个邮箱地址与大量专有信息，比如邮箱系统设定等信息已被窃取。外泄的邮箱地址涉及多个外部组织，包括专家委员会成员的个人电子邮箱。

日本媒体还报道称，东京附近的成田机场也受到事件影响。攻击者设法窃取到机场的空中交通管制数据、航班时刻表与商业运作信息。此外，未授权攻击者也拿到了部分日本外务省数据。日本国土、基础设施、交通与旅游部已经确认了事件的真实性。目前各方已经及时收到提醒通知。

针对本次事件，日本国家网络安全中心先后发布多份公告，警告各使用富士通工具的政府机构及关键基础设施组织立即开展自查，核对是否存在未授权访问及信息泄露迹象。



富士通公司已经紧急叫停其 ProjectWEB 门户，同时全面调查此次事件的影响范围与发生原因。由于 ProjectWEB 门户托管在“soln.jp”域名之上，因此大家可以在网络日志中查找此域名或上述 URL 记录，借此确定组织或客户是否受到影响。

目前尚不清楚这次事件属于漏洞利用还是针对性供应链攻击，相关调查正在进行当中。（来源：互联网内参）