国盟信息安全通报

2019 年 9 月 16 日第 201 期

国盟信息安全通报

（第 201 期）

国际信息安全学习联盟

2019 年 9 月 16 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 709 个，其中高危漏洞 241 个、中危漏洞 413 个、低危漏洞 55 个。漏洞平均分值为 5.85。本周收录的漏洞中，涉及 0day 漏洞 359 个（占 51%），其中互联网上出现“YouPHPTube 远程代码执行漏洞、ASUS SmartHome Gateway HG100 拒绝服务漏洞”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 3140 个，与上周（2022 个）环比增长 55%。

主要内容

一、概述 4
二、安全漏洞增长数量及种类分布情况 4
➢漏洞产生原因（2019 年 9 月 02 日—2019 年 9 月 16） 4
➢漏洞引发的威胁（2019 年 9 月 02 日—2019 年 9 月 16） 5
➢漏洞影响对象类型（2019 年 9 月 02 日—2019 年 9 月 16） 5
三、安全产业动态 6
➢共筑网络安全防线 习近平这样说 6
➢儿童个人信息网络保护的中国良方 8
➢建立工业互联网多层次安全保障体系 有效应对新型安全挑战 11
➢2018-2019 中国信息安全从业人员现状调研报告 13
四、政府之声 21
➢网信办就《网络生态治理规定(征求意见稿)》公开征求意见 21
➢教育部等八部门关于引导规范教育移动互联网应用有序健康发展的意见 22
➢工信部公开征求对《工业大数据发展指导意见（征求意见稿）》的意见 26
➢科技部印发《国家新一代人工智能创新发展试验区建设工作指引》通知 27
五、本期重要漏洞实例 29
➢关于 Microsoft 远程桌面服务存在远程代码执行漏洞的安全公告 29
➢WordPress photo-gallery 插件跨站脚本执行漏洞 30
➢D-link DIR-806 代码注入漏洞 31
➢Cisco Webex Teams 日志功能命令执行漏洞 31
六、本期网络安全事件 32
➢雅虎发生全球宕机：邮箱、搜索等服务都无法正常使用 32
➢谷歌同意为非法收集儿童信息支付 1.7 亿美金的罚款 32
➢16 岁少年化身黑客利用系统漏洞盗取公司 80 余万被判 3 年 6 个月 34
➢人气网络漫画 XKCD 论坛遭网络攻击：大量用户数据被盗 36
➢日本收银员"过目不忘" 疯狂盗刷顾客 1300 张信用卡 36
➢国内首例微信支付赎金勒索病毒案一审宣判 “95 后”黑客获刑六年 37

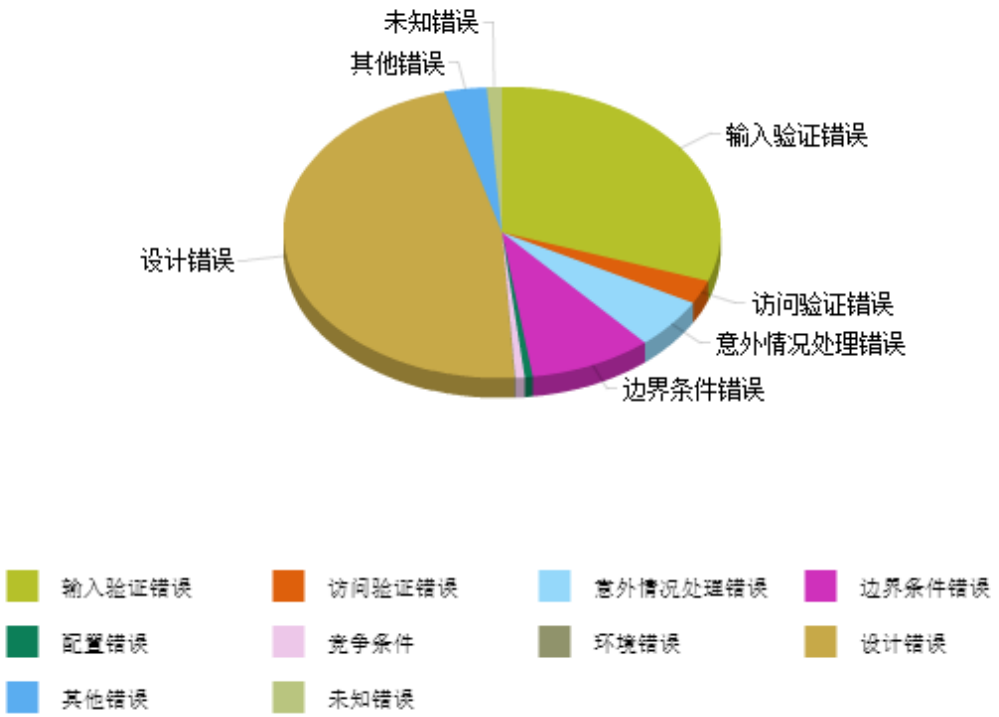
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

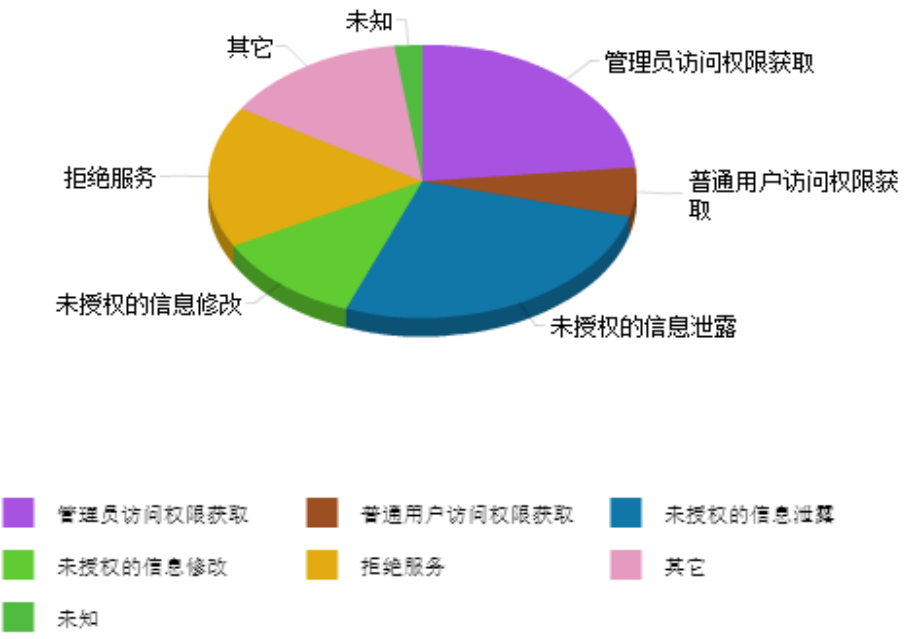
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 709 个，其中高危漏洞 241 个、中危漏洞 413 个、低危漏洞 55 个。漏洞平均分值为 5.85。本周收录的漏洞中，涉及 0day 漏洞 359 个（占 51%），其中互联网上出现“YouPHPTube 远程代码执行漏洞、ASUS SmartHome Gateway HG100 拒绝服务漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3140 个，与上周（2022 个）环比增长 55%。

二、安全漏洞增长数量及种类分布情况

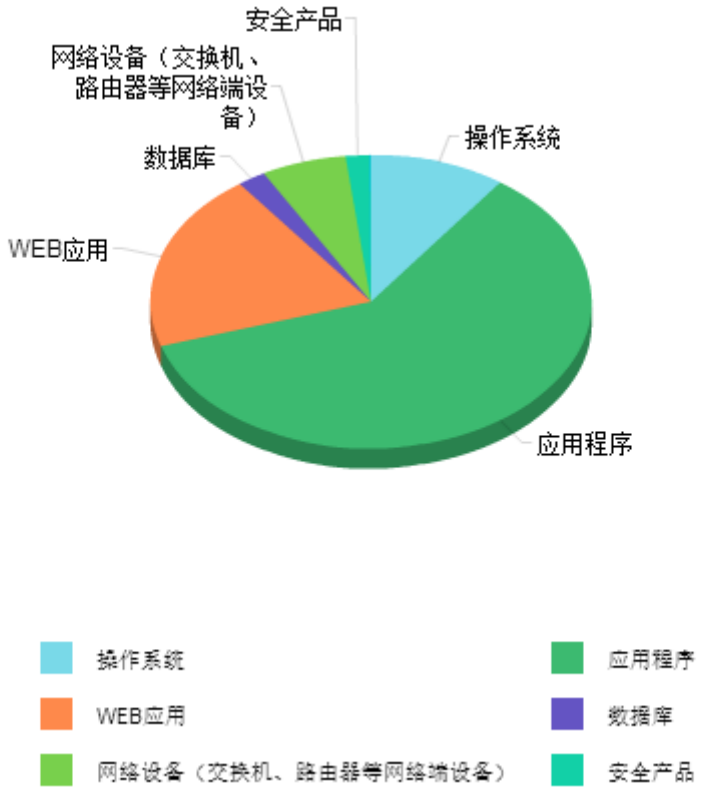
➢ **漏洞产生原因（2019 年 9 月 02 日—2019 年 9 月 16）**



➢ 漏洞引发的威胁（2019 年 9 月 02 日—2019 年 9 月 16）



➢ 漏洞影响对象类型（2019 年 9 月 02 日—2019 年 9 月 16）



三、安全产业动态

➢ 共筑网络安全防线 习近平这样说

2018 年 4 月 20 日至 21 日，全国网络安全和信息化工作会议在北京召开。中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化委员会主任习近平出席会议并发表重要讲话。

2019 年国家网络安全宣传周将于 9 月 16 日至 22 日举行。今年活动的主题为“网络安全为人民，网络安全靠人民”。

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络安全工作，提出了一系列新思想、新理论、新论断、新战略，形成了习近平总书记关于网络强国的重要思想，为做好网络安全工作提供了根本遵循和强大动力。在 2019 年国家网络安全宣传周来临之际，本文特作梳理，与广大网民一同重温总书记相关重要论述，共筑网络安全屏障。

没有网络安全就没有国家安全

在信息时代，网络安全对国家安全牵一发而动全身，同许多其他方面的安全都有着密切关系。

——2016 年 4 月 19 日，在网络安全和信息化工作座谈会上的讲话

没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的

技术，有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济；要有高素质的网络安全和信息化人才队伍；要积极开展双边、多边的互联网国际交流合作。

——2014 年 2 月 27 日，在中央网络安全和信息化领导小组第一次会议上的讲话

维护网络安全不应有双重标准，不能一个国家安全而其他国家不安全，一部分国家安全而另一部分国家不安全，更不能以牺牲别国安全谋求自身所谓绝对安全。

——2015 年 12 月 16 日，在第二届世界互联网大会开幕式上的讲话

中国是网络安全的坚定维护者。中国也是黑客攻击的受害国。中国政府不会以任何形式参与、鼓励或支持任何人从事窃取商业秘密行为。

——2015 年 9 月 22 日，在华盛顿州当地政府和美国友好团体联合欢迎宴会上的讲话

中国愿同各国一道，加强对话交流，有效管控分歧，推动制定各方普遍接受的网络空间国际规则，制定网络空间国际反恐公约，健全打击网络犯罪司法协助机制，共同维护网络空间和平安全。

——2015 年 12 月 16 日，在第二届世界互联网大会开幕式上的讲话

网络安全为人民

2019 年国家网络安全宣传周的吉祥物“津小卫”

网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。

——2014 年 2 月 27 日，在中央网络安全和信息化领导小组第一次会议上的讲话

做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业。

——2014 年 2 月 27 日，在中央网络安全和信息化领导小组第一次会议上的讲话

网络空间是亿万民众共同的精神家园。网络空间天朗气清、生态良好，符合人民利益。网络空间乌烟瘴气、生态恶化，不符合人民利益。

——2016 年 4 月 19 日，在网络安全和信息化工作座谈会上的讲话

保障网络安全，促进有序发展，推动制定各方普遍接受的网络空间国际规则，共同维护网络空间和平安全。

——2015 年 12 月 16 日，在第二届世界互联网大会开幕式上的讲话

网络安全靠人民

网络安全的本质在对抗，对抗的本质在攻防两端能力较量。要落实网络安全责任制，制定网络安全标准，明确保护对象、保护层级、保护措施。

——2016 年 4 月 19 日，在网络安全和信息化工作座谈会上的讲话

要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。

—— 2018 年 4 月 20 日至 21 日，在全国网络安全和信息化工作会议上的讲话

我们要掌握我国互联网发展主动权，保障互联网安全、国家安全，就必须突破核心技术这个难题，争取在某些领域、某些方面实现“弯道超车”。

——2016 年 4 月 19 日，在网络安全和信息化工作座谈会上的讲话

网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。

——2016 年 4 月 19 日，在网络安全和信息化工作座谈会上的讲话

（来源：央视网）

➢ 儿童个人信息网络保护的中国良方

日前，国家互联网信息办公室公布了第 4 号令《儿童个人信息网络保护规定》（以下简

称《规定》），这是我国在儿童个人信息网络保护方面制定的首部专门立法。《规定》全文共二十九条，从儿童个人信息的收集、存储、使用、转移、披露等全生命周期的角度作出了系统全面的规定，同时首次划定了适用的儿童年龄，对儿童及其监护人加强了各项权利保护。《规定》将于 2019 年 10 月 1 日施行，标志着我国儿童个人信息网络保护进入新阶段，对我国儿童个人信息的保护工作具有重要意义。

一、儿童个人信息网络保护为世界性议题

伴随信息通信技术的高速发展，互联网融入了儿童成长的全过程，儿童网民规模和普及率不断攀升。据联合国儿童基金会报告统计，全球网民中未成年人占据了 1/3，每日新增逾 17.5 万儿童网民。中国互联网络信息中心（CNNIC）的数据显示，2018 年 12 月我国未成年网民（6-19 岁）人数占全体网民的 21.6%，总数达到 1.79 亿，互联网普及率高达 93.7%。互联网给儿童提供了诸多正向价值，同时由于儿童的风险防范意识不足，个人信息保护等代表性问题为也给儿童的互联网运用带来了世界性议题。

当前世界各国对于儿童的个人信息保护都十分重视，纷纷采取行动加强儿童个人信息网络保护的立法工作。美国的《儿童在线隐私保护法》（COPPA）、欧盟的《通用数据保护条例》（GDPR）等均对儿童个人信息保护作出了严格规定。

二、《规定》为儿童个人信息网络保护开出中国良方

一是采取更为严格的方式加强保护。相较一般的个人信息的保护，《规定》对适用问题、儿童年龄划分、监护人同意、权利保护、企业义务、执法处罚等作出了明确的专门规定，要

求企业在收集、存储、使用、转移、披露儿童个人信息时相较非儿童个人信息承担更多的义务。

二是对儿童的年龄进行了划分。《规定》将儿童界定为不满 14 岁的未成年人，参考了国内刑事责任年龄的划分和域外的经验做法，结合了儿童身心发展的实际情况，也与现有的推荐性行业标准保持了一致，较好的平衡了权利保护和产业发展。

三是强化对儿童及监护人的赋权保护。《规定》在上位法《网络安全法》的基础上，强化了国际社会已经形成广泛共识的信息权利，如获知信息权（第十条）、更正权（第十九条）、删除权（第二十条）等，加大了对儿童个人信息权利的保护。

四是使企业义务更加明确和具有操作性。《规定》在透明性要求（第八条、第九条）、企业安全义务（第八条、第十二条、第十三条、第十四条、第十五条、第十六条、第二十二条、第二十三条）、个人信息泄露通知义务（第二十一条）等方面作出了全面、明确的规定，便于企业遵守执行。此外《规定》对无法识别属于儿童个人信息的计算机信息系统自动留存处理信息排除适用（第二十八条），更加宽严相济立足产业发展实际。

五是有效夯实相关主体的责任。在执法主体方面，《规定》明确由网信部门主要负责监管，其他《网络安全法》规定的有关部门如电信、公安等在职责范围内也可进行执法。在法律责任方面，各有关部门可根据《网络安全法》的相关规定采取责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照等行政处罚。

三、我国儿童个人信息网络保护正式步入新阶段

（一）强化立法保护是应有之义

当前加强儿童个人信息网络保护才能更好的回应现实需要。技术进步和产业发展提速推动儿童触网更加普遍，而此前我国儿童个人信息网络保护机制尚不健全，滥采滥用儿童个人信息情况严重，网络空间安全威胁和风险日益突出，儿童的权益保障有待加强。社会各界对加强儿童的个人信息保护形成了广泛共识和呼声，在此形势下《规定》率先出台，强化我国对儿童个人信息网络保护的力度，回应了广大人民群众的关切。

（二）立足本土实际具中国特色

《规定》解决了我国此前面临的儿童个人信息网络保护无专门立法可依的实际问题。《规定》立足上位法基础，参考行业企业在实践中凝练出的相关标准与经验，注重对美国、欧盟等国外立法、研究及实践经验的借鉴吸收，广泛征求社会公众意见，凝聚了广泛的共识，标志着具有中国特色的儿童个人信息网络保护的顶层设计方案正在逐步构建完善。

（三）提升保护水平与美欧接轨

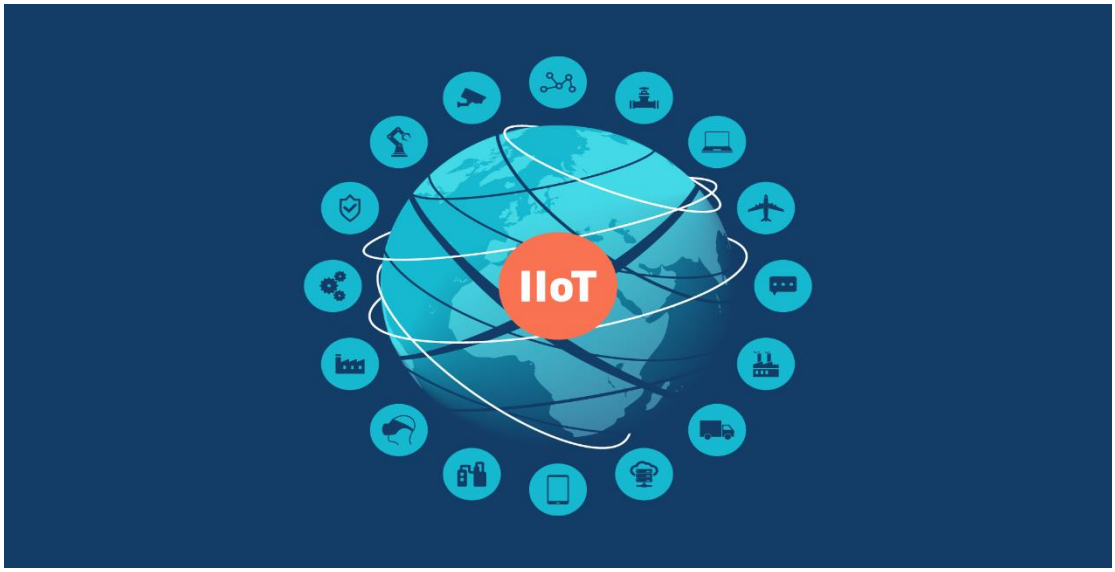
《规定》提升了我国儿童个人信息网络保护的水平，构建了与美国、欧盟等发达国家相接轨的治理体系，也营造国内外水平一致的法律环境，有助于提高我国互联网企业的法律合规意识，为我国在个人信息保护领域国际规则制定方面赢得话语权也贡献了力量。《规定》不仅标志着我国国内的儿童个人信息网络保护水平进入新的阶段，同时也标志着数字经济时代处于领先地位的中国、美国、欧盟都对儿童的个人信息网络保护作出了规定，其中形成共识的制度设计势必将影响更多世界范围内的其他国家携手加强儿童个人信息网络保护。

（四）构建法律体系建长效机制

《规定》作为专门的部门规章，其出台对未成年人个人信息保护的整体法律体系构建具有重要意义。当前《民法典》人格权编二审稿草案强调了加强未成年人的个人信息保护，《个人信息保护法》《未成年人保护法》正在加紧推进起草或修订工作，行政法规层级的《未成年人网络保护条例》也正在有序审议。《规定》为体系化的法律、法规与配套规定的出台及落地实施奠定了良好的前期基础，期待我国未成年人个人信息保护的法律体系的密网早日织就，长效保护机制一并水到渠成。（来源：中国网信网）

➢ 建立工业互联网多层次安全保障体系 有效应对新型安全挑战

近日，工业和信息化部发布了《关于加强工业互联网安全工作的指导意见》（以下简称《指导意见》）的通知，进一步贯彻落实国务院《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，加快构建工业互联网安全保障体系，护航制造强国和网络强国战略实施。



建立工业互联网多层次安全保障体系

工业互联网从生产端入手，能提高供给体系质量和效率，扩大中高端供给，增强供给侧结构对需求变化的适应性，推动传统工业转型升级，让各种资源更加优化配置，推动我国经济朝着更高质量发展；加快新兴产业培育，催生智能化生产、网络化协同、服务化延伸、个性化定制的诸多新产业。

国务院《关于深化“互联网+先进制造业”发展工业互联网的指导意见》中将安全保障与网络、平台建设共列，成为工业互联网的三大体系之一，提出建立工业互联网多层次安全保障体系。

2018 年被业界称为工业互联网“元年”。6 月，工信部组建中国工业互联网研究院。7 月，信息化部印发了《工业互联网平台建设及推广指南》和《工业互联网平台评价方法》。2019 年 1 月 18 日，工信部印发了《工业互联网网络建设及推广指南》。3 月，“工业互联网”成为“热词”并写入《2019 年国务院政府工作报告》。工业互联网近些年逐渐在全球范围内受到了主要国家的高度重视。

但工业互联网在世界范围内仍然是一个新兴技术，正处在蓬勃发展当中。当前，工业互联网的安全问题基本由工业企业的安全问题催生而来。

坚持发展与安全并重 有效应对新型安全挑战

《指导意见》指出要落实企业主体责任、政府监管责任，围绕设备、控制、网络、平台、数据安全构建工业互联网安全保障体系，对企业实施分类分级管理，坚持发展与安全并重，安全和发展同步规划、同步建设、同步运行，最终形成工业互联网安全事前防范、事中监测、事后应急能力。同时鼓励推动重点领域技术突破，加快安全可靠产品的创新推广应用，有效应对新型安全挑战。

《指导意见》规划，到 2020 年底，从制度机制、技术手段、产业发展三个方面，初步建立我国的工业互联网安全保障体系。到 2025 年，制度机制健全完善，技术手段能力显著提升，安全产业形成规模，基本建立起较为完备可靠的工业互联网安全保障体系。

五大举措应对工业互联网安全

那么，企业和政府如何应对工业互联网安全？

一是企业和政府依法按照“谁运营谁负责，谁主管谁负责”的原则，企业明确落实工业互联网主体责任，政府明确落实监督管理责任。

二是政府构建工业互联网安全管理体系，国家级政府部门支持专业机构、企业积极参与相关国际标准制定，建立分类分级管理机制、建立工业互联网安全标准体系。地方政府部门

依据工业互联网安全管理体系，监督和指导企业开展工业互联网安全工作，健全安全管理制度。在 2020 年底制定设备、平台、数据等至少 20 项亟需的工业互联网安全标准，探索构建工业互联网安全评估体系。

三是企业依照政府构建的工业互联网安全管理体系强化安全防护能力。围绕设备、控制、网络、平台、数据安全加强自身安全防护能力，推动工业企业、工业控制系统生产企业、工业互联网集成商和工控安全服务商加强合作，提升工业互联网的本质安全。同时企业依托工业互联网安全攻防演练环境，在工业互联网平台和工业 APP 上线前对其进行安全评估和检测，针对平台各层分层部署安全防护措施；在平台和 APP 上线后，建立风险评估、安全审计等机制，保障工业互联网安全稳定运行；建立工业互联网全产业链数据安全管理体系，加强工业互联网重要数据安全监测和管理，完善重大工业互联网数据泄露事件触发响应机制。

四是政府支持工控安全企业的科技创新，支持专业机构、高校、企业等联合建设工业互联网安全创新中心和安全实验室，促进工业互联网安全产业发展。在重点行业开展试点示范，加强工业企业和工控安全企业的合作，打造产学研用协同创新发展平台。最终在 2020 年底形成至少 20 个创新实用的安全产品、解决方案的试点示范，培育若干具有核心竞争力的工业互联网安全企业。

五是政府部门建设国家、省、企业三级协同的工业互联网安全技术保障平台、建立工业互联网安全基础资源库、建设工业互联网安全测试验证环境。这也是对《工业控制系统信息安全行动计划（2018-2020 年）》中提到的“一网一库三平台”的延伸。在 2020 年底基于这些基础库，政府开展工业互联网安全评估认证，提升工业企业、工业控制系统生产企业、工业互联网集成商和工控安全服务商的安全防护水平，最终提升安全公共服务能力。

最后，《指导意见》还提出一系列的保障措施来确保《指导意见》的贯彻执行。（来源：人民网）

➢ 2018-2019 中国信息安全从业人员现状调研报告

网络空间的竞争，归根结底是人才竞争。新一轮科技革命和产业升级进程中，信息技术正在从根本上改变人们生产生活的方式，重塑经济社会发展和国家安全的新格局，信息安全人才将在这一转型发展过程中发挥关键作用。面对新时期的挑战和机遇，能否有效推进信息安全人才建设将成为实施网络强国战略至关重要的因素，也是在日益激烈的国际竞争中赢得

主动的关键所在。

党的十八大以来，国家就网络安全人才发展做出一系列重要部署，推出多项有力措施，取得了有目共睹的成就。网络安全学科专业设置、院系建设、学历教育方面取得突破性进展；网络安全在职培训和专业资质测评快速推进；网络安全攻防演练和技能竞赛蓬勃发展；多地规划建设网络安全人才和创新基地，出台人才培养和引进政策；重要行业严格落实网络安全责任制和人员合规要求，加快实施安全人员培训和管理制度；相关部门深入开展宣传教育，全社会网络安全意识得到显著提升。

我国正处于信息安全人才发展的重大战略机遇期。当前和未来一段时期有必要通过深度调研，持续跟进信息安全从业人员队伍现状，探索信息安全人才成长规律，分析人才队伍建设中存在的深层次问题。“中国信息安全从业人员现状调研（2018-2019 年度）”是由中国信息安全测评中心主办，中国信息产业商会信息安全产业分会承办的大型调查活动。本报告通过在线问卷调查、一线实地访谈、专家会商研讨等方式，从六大维度深度调研信息安全从业人员及当前人才环境现状，以期为广大安全从业人员提供职业发展指导，为安全行业人才工作创新发展提供实践指引，为国家网络与信息安全人才队伍建设提供决策参考。

一、主要调研结果

本调研报告从调研对象、工作状况、流动配置、能力提升、制度环境、安全态势六个维度深入分析信息安全从业人员及当前人才环境现状，对备受关注的从业人员群体划分、教育培训、考核评价、激励保障、队伍建设、人才相关政策法规落实等内容进行了全面覆盖。

（一）调研对象

报告首次对信息安全这一非传统领域的从业人员进行定义和分类，将调研对象明确为“以信息安全工作职责为主要社会劳动分工和生活来源的人员”，并把信息安全从业人员工作角色分为 6 个大类，14 个子类。调研显示，当前承担安全运营（62.4%）和安全建设（32.4%）工作角色的信息安全从业人员数量最多；45.5%的从业人员在私营企业任职，其次为国有企业（19.3%）和政府机关事业单位（16.5%）；近四成（38.4%）从业人员都参加过实战类网络安全竞赛。

（二）工作状况

一个单位是否建立有数量充足的专业信息安全团队是安全工作是否到位的重要指标。调研数据显示，除信息安全专业服务企业、特大型企业集团，以及大型互联网企业建立有较大规模的信息安全人才梯队外，50%的政企单位信息安全团队人员规模在 20 人以下；近六成信息安全从业人员需要承担非信息安全内容的工作，政府机关事业单位信息安全工作人员“身兼数职”现象最显著；各种类型的人才均存在短缺现象，其中承担安全建设和规划管理类工作角色的人才相对更加紧缺。

（三）流动配置

信息安全从业人员平均年薪约为 15.3 万元，同上一年度相比薪酬继续上涨，但增幅有所缩减；42.9%的信息安全从业人员工作压力感受明显，但对职业发展前景多持乐观态度；过去三年人才流动速度放缓，影响职业流动的原因依次是“薪酬”、“晋升空间”、“工作氛围”和“自我价值实现”，显示从业人员对工作的福利性因素和发展性因素均十分看重。

（四）能力提升

本次调研中，“职业培训”取代上一年度的“自我学习”成为信息安全从业人员最倾向于选择的能力提升方式（68.8%）；从业人员在各细分方向均存在能力提升需求，排名靠前的依次是大数据安全、云安全、安全管理和渗透测试；在各类信息安全证书中，从业人员持有最多（71.8%）、最希望获取（68.9%）注册信息安全专业人员（CISP）资质证书。

（五）制度环境

专人专岗从事专门工作是职业化的一种体现。近七成信息安全从业人员所在单位设置了专门的网络安全管理部门和负责人，但其中 57.7%的人员需兼任其他非安全类工作，“人岗不匹配”的现象比较普遍；65.5%的从业人员所在单位设有职业晋升通道和工作激励机制，但认为相关机制“实施效果良好”的人群占比不足两成；43.7%的从业人员认为自己没有清晰的职称序列归属，同上一年度（25.9%）相比明显增加；63%的从业人员在入职前需经过一

定形式的背景调查。

（六）安全态势

从业人员工作中最经常面对的信息安全威胁依次是漏洞攻击、数据泄露和拒绝服务攻击；发生信息安全事件最主要的原因是管理不完善、缺乏安全培训、管理层不重视，以及人才和资金不足；78.0%的人员所在单位制定了内部网络安全管理制度和操作规程，但仅四分之一人员反馈实施效果良好；77.6%的从业人员所在单位都已开展了信息安全风险评估工作；“芯片”取代上一年度“操作系统”成为受访者眼中最应国产化的核心技术。

二、存在的问题

网络与信息安全人才是民生急需和战略必争领域的重要资源，信息安全人才队伍建设是保障国家网络空间安全的重要基础性工作。近年来我国信息安全人才队伍建设工作取得了突破性进展，但应看到当前的人才队伍能力结构同经济社会发展和国家安全需求仍存在较大差距。本次调研显示，当前我国信息安全人才队伍建设还存在以下突出问题。

（一）信息安全从业人员全方位短缺

信息安全工作贯穿信息化建设的各个环节，无论是在数据、应用、系统、网络等工作层面，还是涉及到研发、建设、运营、管理、生产等业务流程，都需要有人承担信息安全职责。但目前我国信息安全从业人员整体呈现全方位短缺的态势，一是信息安全人员规模总量不

足，除信息安全专业服务企业、特大型企业集团，以及大型互联网企业建立有规模化的信息安全人才梯队外，50%的政企单位信息安全团队人员规模在 20 人以下；多数受访者认为自己所在单位的信息安全人员队伍规模无法满足当前工作需要。二是大量信息安全工作以“非专职”方式完成，近六成信息安全从业人员需要承担非信息安全内容的工作，政府机关事业单位里需要“身兼数职”的现象最为显著；在需要兼职非安全工作的人群中，33.8%的受访者承担的非安全工作在日常工作中占比超过 50%。三是各类安全工作角色均存在人才缺口，从安全角色大类来看，安全建设和规划管理类的角色相对更加紧缺；从子类来看，最紧缺的角色依次是分析设计、组织管理、开发与集成；受访者普遍认为，信息安全人才资源不足是造成信息安全事件最重要的原因之一。

（二）信息安全职业化尚处于初级阶段

信息安全职业化指的是对信息安全从业人员专业知识、能力和行为准则进行标准化规范，职业化的一个体现是由专人专岗负责专门工作。我国《网络安全法》已对关键信息基础设施运营者“设置专门安全管理机构和安全管理负责人”做出了明确规定，同时鼓励其他网络运营者自愿参与关键信息基础设施保护体系。调研显示，近七成信息安全从业人员所在工作单位已设置了专门的网络安全管理部门和负责人，但目前信息安全的职业化总体来看还处在发展初级阶段。一是信息安全目前还没有统一的职业（族）标准，对从业人员如何分级分类、应具备何种专业知识和能力水平等问题尚未建立标准规范，各用人单位的信息安全岗位设置和能力要求各行其是，差别较大。二是信息安全“人岗不匹配”情况普遍，近七成信息安全从业人员所在工作单位设置了专门的网络安全管理部门和负责人，但在已建有此机制的单位中仍有 57.7%的从业人员需要兼任其他非安全类工作，“人岗不匹配”的现象仍比较普遍，有的从业人员专业能力达不到岗位要求；有的岗位名为信息安全专岗，但在岗人员从事的实为信息化等工作。三是社会对信息安全职业意识普遍不强，尤其是用人单位高层，或是对信息安全工作以及信息安全人才重要性的认知有待提升，或是对人才工作的重要性只有原则上的认同，在如何科学有效地加强信息安全队伍建设方面缺乏工作抓手；超过一半的从业人员认为行政管理高层对信息安全工作不重视是安全事件发生的主要原因之一。

（三）人员能力提升需求难以得到满足

人才是第一资源。战略性的人力资源管理核心在于把人看作重要的资产，通过教育培训等投入，持续提高其知识、技能和素质水平，更好地达成用人单位的业务目标。用人单位能否提供足够的培训、持续提升人才专业能力、帮助其完成自我价值实现，将在“引才”和“留才”中发挥越来越重要的作用。当前人员能力提升需求普遍难以得到满足，一是从业人员能

力提升需求旺盛，新入职人员在学历教育之后普遍需要进行“二次培训”，已从业的人员也需要持续教育和终身学习。调研显示，受访者在专业知识和能力的各个细分方向均有能力提升需求，其中最希望提升的是大数据安全、云安全、安全管理和渗透测试等方向的专业能力。二是从业人员期望获得专业资质，作为证明自己具备一定知识、能力和工作经验的凭证。超过六成（64.7%）的受访者持有不同类型的信息安全资质证书，其中持有注册信息安全专业人员（CISP）资质证书的占比最高（71.8%）。未来一年内，有 83.7%的从业人员期望获得信息安全资质证书，其中希望获取 CISP 证书的人员占比最高，达到 68.9%。三是用人单位教育培训投入不够，对信息安全人员普遍存在“使用多、培养少”的情况，内训制度实施效果不佳，74.9%的从业人员所在单位建立了信息安全工作人员培训制度，但仅有 23.1%的受访者认为培训取得了良好效果；同时，用人单位资助从业人员接受职业培训的意愿和力度也不高，资助比例达到 50%以上的占比仅为 18.5%，33.5%的从业人员表示自己所在工作单位不提供任何资助。

（四）信息安全人才体制机制存在障碍

网络与信息安全作为跨界、交叉、融合的非传统行业，唯有在鼓励创新发展的体制机制下，才能让人才的创造活力竞相迸发、聪明才智充分涌流。当前信息安全人才发展还存在一系列制度性障碍，一是对安全从业人员考核评价手段不足，信息安全工作不易直接量化考核，信息安全成果和价值难以直接得到体现。43.7%的信息安全从业人员认为自己没有清晰的职称序列归属，大量体制内信息安全从业人员在职称评审、考核评价或选拔任用时存在困难。二是人员鼓励激励机制不健全，职业上升空间有限。65.5%的信息安全从业人员表示其所在工作单位的人事管理部门建立了针对信息安全从业人员的职业晋升通道和工作激励机制，但认为相关机制“实施效果良好”的人群占比不足两成。三是缺乏向重要关键领域的人才引导机制，从业人员在职业流动中对福利性因素和发展性因素均十分看重，但当前大量关键信息基础设施运营单位在“待遇引人”、“事业留人”等方面均面临挑战，甚至自有人才流失的现象也比较严重。

三 、对策建议

新时代落实网络强国战略部署，要求我们必须以习近平新时代中国特色社会主义思想特别是网络强国战略思想为指导，把人才工作摆在更加突出的战略位置，进一步提高信息安全人才工作的重要性和紧迫性，利用大国优势和制度优势，把提升全社会信息安全意识和能力、尤其是提升信息安全从业人员专业能力的工作推向前进。结合从业人员现状，本报告对信息安全人才队伍建设提出以下建议。

（一）建立体系化的信息安全人才发展规划

从提高信息时代生产力的高度，以建设具有全球竞争力的网络安全人才队伍为目标，对国家网络与信息安全人才发展全局进行系统性的超前规划部署，争取主动局面，为信息安全专业人才队伍建设夯实基础、提供土壤。一是构建网络安全国民教育和持续教育体系，为各类网络安全意识提升、基础教育、高等教育、职业培训、持续教育提供总体指导，为包括信息安全从业人员、后备人员以及普通公众在内的社会全体成员信息安全能力、防护技能的提升提供支撑。二是统筹推进网络安全人才发展整体工作，通盘规划信息安全人才培养、管理和使用等各项工作，明确主要任务和阶段性目标，加快信息安全人才管理体制以及人员流动配置、培养开发、考核评价和激励保障等工作机制改革。三是多主体协同共建网络安全人才生态，提高相关主管领导部门、产业界、学术界、科研院所、用人单位等相关各方的支持配合力度，有力整合资源，完善配套措施，形成推进合力，共同构建良好的网络与信息安全人才发展生态。

（二）科学推进信息安全人才的职业化发展

在信息安全从业人员全方位短缺的严峻形势下，职业化手段有助于明确信息安全职业的正当性、改进信息安全教育培训的针对性、促进信息安全人才供需匹配、提升信息安全职业吸引力。但作为新兴的非传统领域，信息安全的职业化不宜对不同类型从业人员简单采用“一刀切”的职业许可方式进行管理。建议，一是要深入开展信息安全人才发展基础理论和前沿实践研究，探寻信息安全人才成长规律，形成科学的信息安全从业人员测评标准，作为安全人才职业化的发展依据，为制定人员教育培训目标、完善人才管理体系提供支撑。二是要建立兼具相对稳定性和动态灵活性的信息安全知识体系，综合信息安全专业能力图谱中核心和通用的部分，维持一个相对稳定的基础知识体系；针对细分方向和前沿领域的部分，建立动态调整的知识子域，为信息安全职业化夯实基础。三是要推进权威机构的信息安全专业人才资质认定工作，有公信力的机构开展资质认定工作能够有效证明从业人员具备了相应的专业知识和能力、工作经验和业绩、以及较高的职业道德水平，从而为信息安全人才评价考核、选拔任用、职业晋阶提供参考依据。

（三）着力提升信息安全从业人员规模能力

以经济社会发展和国家安全需求为导向，加强人才培养体系建设工作的前瞻性和针对性，建立贯穿信息安全从业人员学习工作全过程的终身教育制度，提高信息安全人才队伍的数量规模和整体能力。一是加大教育培训投入和工作力度，既要利用好成熟的职业培训体系，快速培养信息安全急需人才；也要在基础教育、高等教育和职业院校中深入推进网络安全教育，

积极培养信息安全后备人才；全面优化教育培训的内容、类别、层次结构和行业布局，着力解决信息安全人才总量不足的突出问题。二是分类施策建设信息安全人才梯队，对于社会对信息安全基层人员的需求，开展规模化培养，尽快解决当前用人需求；对于卓越工程师和高水平研究人才的需求，在工程和科研项目基础上加强专业化培训，打造信息安全攻坚团队和骨干力量；对于信息安全核心技术人才和特殊人才的需求，探索专项培养选拔方案，塑造信息安全核心关键能力。三是结合领域特点推进信息安全教育培训供给侧改革，加强专业资质测评在人才队伍建设中的引领和导向作用，创新人才培养模式，深化产教融合，贯通后备人才到从业人员的通道，推动各类学校、专业培训机构和企业通过校园教育、现代学徒制培训、任职培训、在职培训、岗位练兵、攻防竞赛、技术比武等方式，推动信息安全人才工作的高质量发展。

（四）持续优化信息安全人才发展整体环境

网络安全是信息技术的尖端领域，是智力最密集、最需要创新活力的领域。坚持以用为本、急用先行的原则，加快信息安全人才发展体制机制创新，制定适应信息安全特点的人才政策，让人才的创造活力竞相迸发，聪明才智充分涌流。一是提高各级党政领导干部的网安意识和网安人才意识，在干部培训中将网络安全作为必修课程，引导其积极适应时代要求，强化网络安全思维，提高对人才工作重要性的认识，真正尊重人才、爱才惜才，为人才发展创造良好条件。二是加快创新信息安全从业人员评价激励机制，参考企业中激发信息安全人才活力效果最好的管理实践和经验，创新发展适应信息安全特点的薪酬制度、评价指标和鼓励激励措施，让信息安全人才价值得到尊重和体现，名正言顺地提高从业人员的经济待遇和社会地位。三是建立重点领域信息安全人才引导和优先保障机制，采取特殊政策，完善配套措施，引导和鼓励信息安全人才向国家党政机关、要害部门、重要行业、关键信息基础设施运营单位流动，确保重点领域能够招得进、用得好、留得住信息安全高端人才和紧缺人才。

（来源：《中国信息安全》杂志）

- **中国信息安全从业人员现状调研报告（2018-2019 年度）**
- **全文：**http://www.itsec.gov.cn/zxxw/201909/P020190906557330247920.pdf

四、政府之声

➢ 网信办就《网络生态治理规定(征求意见稿)》公开征求意见

2019 年 9 月 10 日，国家互联网信息办公室就《网络生态治理规定（征求意见稿）》向社会公开征求意见。意见反馈截止时间为 2019 年 10 月 10 日。

征求意见稿明确，网络信息内容生产者不得制作含有带有性暗示、性挑逗、性诱惑的；展现血腥、惊悚等致人身心不适的；宣扬炫富拜金、奢靡腐化等生活方式的；过度炒作明星绯闻、娱乐八卦的；使用夸张标题，内容与标题严重不符等内容的不良信息。

对于网络信息内容服务平台，征求意见稿提出应当切实履行网络生态治理主体责任，加强本平台生态治理工作。网络信息内容服务平台采用个性化算法推荐技术推送信息的，应建立健全人工干预机制，建立用户自主选择机制。同时，还应当在首页、账号页面、信息内容页面等显著位置设置便捷投诉举报入口。

关于网络信息内容服务使用者，征求意见稿要求，在以发帖、回复、留言、弹幕等形式参与网络活动时，积极弘扬正能量，不得复制、发布、传播违法信息，自觉抵制不良信息。不得利用网络和相关信息技术，实施侮辱、诽谤、威胁以及恶意泄露他人隐私、散布谣言、人肉搜索等网络侵权、网络暴力行为，侵害其他组织或者个人合法权益。此外，还规定不得通过人力或者技术手段实施流量造假、流量劫持以及虚假注册账号、批量买卖账号、操纵用

户账号等行为，破坏网络生态秩序。

“网信部门根据相关法律法规规定，会同有关部门建立健全网络信息服务严重违规失信联合惩戒机制。”征求意见稿还指出，对严重违反规定的网络信息内容服务平台、网络信息内容生产者和网络信息内容使用者依法依规实施限制从事网络信息服务、网上行为限制、行业禁入等惩戒措施。（来源：中国网信网）

- **《网络生态治理规定（征求意见稿）》**
- **全文：**http://www.cac.gov.cn/2019-09/11/c_1569729939897372.htm

➢ 教育部等八部门关于引导规范教育移动互联网应用有序健康发展的意见

2019 年 9 月 5 日，教育部等八部门印发《关于引导规范教育移动互联网应用有序健康发展的意见》（以下简称《意见》）。为此，教育部科学技术司负责人就有关问题回答记者提问。

1.请简要介绍《意见》制定出台的背景？

《意见》制定出台主要有以下三方面的背景。

一是落实党中央国务院的决策部署。党中央、国务院高度重视“互联网+教育”。习近平总书记在网络安全和信息化工作座谈会上提出实施“互联网+教育”，促进基本公共服务均等

化，让亿万人民在共享互联网发展成果上有更多获得感。李克强总理在 2019 年政府工作报告中指出发展“互联网+教育”，促进优质资源共享，发展更加公平更有质量的教育。教育 App 是“互联网+教育”的重要载体，规范教育 App 管理是促进“互联网+教育”发展的重要内容。

二是回应人民群众的关切和期盼。近几年，教育 App 快速发展、广泛应用，对“互联网+教育”发展发挥了积极作用。但一些地方和学校出现了应用泛滥、平台垄断等现象；一些教育 App 存在有害信息传播、广告丛生等问题，给广大师生带来了困扰，增加了学生和家长的负担。媒体对此多有报道，反映问题较为尖锐，加强教育 App 治理的呼声十分强烈。

三是深化“互联网+教育”发展的内在需求。2018 年，教育部印发文件，对中小学学习类 App 乱象进行了集中治理。随着工作深入，不止中小学学习类 App 需要规范，学校管理、服务等工作的教育 App 也需要引导规范。教育系统迫切需要出台一个较全面、有力度的文件加强对教育 App 发展的统筹指导，产业界也热切期盼出台政策明确监管标准，为教育 App 有序健康发展营造良好氛围。

2.请简要介绍《意见》制定起草的过程？

《意见》从今年 2 月开始起草，到 8 月印发历时近半年，过程分为三个阶段。

一是加强学习领会。学习贯彻习近平总书记关于教育和关于网络强国的系列重要讲话精神，全面落实全国教育大会精神、全国网络安全和信息化工作会议精神，特别是贯彻落实好中央领导同志关于规范教育 App 管理的指示批示精神。认真研究关于民办教育、App 管理的相关法律法规和政策文件，明确政策出发点和法律法规要求。

二是深入调查研究。今年 3 月，开展了教育 App 的专项调研，抽取了 300 家教育行政部门和学校（其中高校 100 所，教育部直属单位 10 个，教育行政部门 62 个，职业院校、中小学 128 个），调研教育 App 的发展和应用状况。收集人民网、新华网、中国青年报、南方都市报等新闻媒体关于教育 App 的报道，系统梳理教育 App 存在的问题，针对问题逐一研究，拿出切实可行的解决措施，回应社会关切。

三是广泛征求意见。与中央网信办、工业和信息化部、公安部、民政部、市场监管总局、国家新闻出版署、全国“扫黄打非”办等部门保持密切联系，共同研究具有可操作性的政策措施。征求省级教育行政部门、有关高校的意见，召开企业座谈会，听取 30 家教育 App 提供者、App 分发平台、移动终端制造者的意见，保障各项政策措施可落地，有效果。

3.请问《意见》和《教育部办公厅关于严禁有害 App 进入中小学校园的通知》、《教育部等六部门关于规范校外线上培训的实施意见》是什么关系？

答：三个文件都是贯彻落实习近平总书记关于教育的系列重要讲话精神，落实全国教育大会精神，发展“互联网+教育”，办好网络教育的重要举措。教育部密集部署体现了部党组对“互联网+教育”的高度重视，体现了以人民为中心的发展思想。总的来说，三个文件在指导思想上同向同行，但职责任务上各有侧重。

相比于《教育部办公厅关于严禁有害 APP 进入中小学校园的通知》治理中小学学习类 App，《意见》所涉及范围更广，不止于中小学，也不局限于学习类 App，是一个全口径的文件。相比于《教育部等六部门关于规范校外线上培训的实施意见》规范中小学校外线上培训机构，《意见》不止于中小学，也不局限于校外。同时，教育 App 只是校外线上培训的载体之一，而校外线上培训也只是教育 App 承载的内容之一。

三个文件促进“互联网+教育”发展的导向是一以贯之的，但不同阶段政策侧重点不同。短期靠专项行动治理乱象、中期靠制度建设规范管理、长期靠提高质量满足学生需求。2018 年，教育 App 反映的问题较为集中，在此背景下，教育部出台文件治理乱象，有效抑制了中小学学习类 App 存在的突出问题。随着工作不断深入，教育部因势利导出台《意见》，从更长远的角度促进教育 App 有序健康发展。

三个文件规范教育 App 管理的决心也是一以贯之的。规范是为了更好地发展，只有让教育 App 在法治、有序的轨道上发展，才能真正促进教育 App 的有序健康发展。教育部将一如既往地坚持人民为中心的发展思想，治理教育 App 乱象，规范教育 App 管理，促进优质教育 App 发展，切实维护广大师生和家长的切身利益。

4. 《意见》提出建立备案制度的考虑是什么？将如何执行？

答：备案制度是《意见》明确的一项重要制度，是规范教育 App 管理的基础。关于备案制度的相关情况如下。

一是建立备案制度的考虑。根据国务院“放管服”改革精神，对于新兴产业实施包容审慎监管。2016 年，国务院印发《关于第二批取消 152 项中央指定地方实施行政审批事项的决定》，明确取消网站网校审批许可。2017 年，教育部印发《关于教育网站网校审批取消后加强事中事后监管工作的通知》，明确了教育 App 监管的方向。教育部建立备案制度，目的是准确掌握教育 App 供需双方情况，做到底数清、情况明，为事中事后监管提供支撑。同时，根据大数据分析掌握教育 App 发展现状和存在问题，为引导规范教育 App 有序健康发展提供决策依据。

二是落实备案制度的考虑。教育 App 的备案按照“国家统一标准、各省分头实施、企业属地备案”的原则开展。国家统一标准，即教育部制定教育 App 备案管理办法，明确备案主

体、备案时间、备案内容和备案流程。各省分头实施，即以省为单位推动备案，由省级教育行政部门组织本地区的教育 App 提供者和教育机构进行备案。企业属地备案，即教育 App 提供者为企业的到注册地的省级教育行政部门进行备案，通过信息共享实现“一省备案，全国有效”。教育 App 提供者为学校的，按照隶属关系到所属教育行政部门备案。

根据国家“放管服”改革精神，教育部依托国家教育资源公共服务平台为备案工作提供信息化支撑，实现全程网上办理。通过数据共享全面简化备案所需提供的材料，方便企业和学校备案，为他们提供优质服务。备案结果网上公示，公众和机构均可查询，为社会监督提供便利。

5.《意见》将采取什么措施解决 App 泛滥的问题？

答：为切实治理教育 App 泛滥等问题，教育部将于近期启动专项行动，从以下方面加强统筹管理、治理应用乱象：一是加强教育 App 开发的统筹管理。学校行政部门或教师开发教育 App 并要求学生使用的，需经学校批准立项，不得擅自开发。二是加强教育 App 选用的统筹管理。选用教育 App 要充分征求师生、家长意见，并经领导班子集体决策同意。三是加强教育 App 整合共享的统筹管理。严格控制本单位教育 App 的数量，同一业务、不同层次不得开发多个 App。四是加强教育 App 数据的统筹管理。采集个人信息应遵循最小化原则，大范围采集个人信息应经领导班子集体决策同意，第三方 App 采集个人信息应与学校签订数据安全协议。不得向用户重复采取个人信息，严格限制采集个人生物识别信息。

广大师生、家长答应不答应、高兴不高兴、满意不满意，是检验治理教育 App 泛滥成效的根本标准。在治理过程中，教育部将注重典型示范，鼓励教育行政部门和学校以清理促整合，以规范促发展，切实优化师生应用体验，切实营造教育 App 发展的良好环境。

6.《意见》将采取什么措施规范教育 App 的商业行为，以解决广告泛滥，利益裹挟、应用垄断等问题？

答：《意见》对于规范商业行为提出了明确的要求，归纳起来就是：“强制的不商业，商业的不强制”。强制的不商业，即作为教学、管理工具要求统一使用的教育 App，不得向学生及家长收取任何费用，不得植入商业广告和游戏。商业的不强制，即推荐使用的教育 App 应当遵循自愿原则，不得与教学管理行为绑定，不得与学分、成绩和评优挂钩。

规范教育 App 的商业行为，需要处理好教育事业民生属性和教育移动应用市场属性之间的关系。下一步，教育部将按照“疏堵结合、标本兼治”的原则做好相关工作：一是在国家教育资源公共服务平台上设置渠道，接受群众投诉举报，同时加强对相关舆情的监测，根据问题线索加强对广告泛滥、利益裹挟、应用垄断等问题的监管。二是加强行业自律，建立

行业信用评价体系和服务评议制度，指导教育 App 提供者自觉遵守进入校园的规范。三是鼓励学校探索购买优质教育 App 服务，推动学校深入应用，不断优化教育 App 的供给方式，提高资源和服务的供给质量，为教育 App 相关企业发展创造良好的市场环境，找到一个双赢的发展模式。

7.请问教育部将如何做好教育 App 的监管工作？

答：根据《意见》的要求，将从以下三方面做好教育 App 的监管工作。

一是加强标准规范制定。《意见》在广泛调研的基础上，明确教育 App 监管的标准，从内容管理、数据规范和安全保障等方面划出了红线、指明了方向。教育 App 仍处于发展期，对教育 App 的认识也在不断深化，下一步教育部将会同有关单位研究制定教育 App 的标准规范，细化落实工作要求。

二是开展常态化监管。教育部将加强和职能部门、专业机构、行业协会、企业的合作，建立常态化的监测通报和预警机制。及时发现、通报安全隐患，督促整改和反馈。基于隐患修复和投诉举报信息，建立信用监管机制。对具有良好信用记录的教育 App 减少检查次数；对有不良信用记录的教育 App 增加检查次数，让守信者无事不扰、失信者时时不安。

三是做大监管同心圆。贯彻落实“互联网+监管”的要求，会同网信、电信、公安、市场监管、扫黄打非等部门实施联合监管。加强行业自律，发挥教育 App 提供者、App 分发平台、移动终端制造商等主体的作用，规范行业管理。建立扁平化的意见反馈和投诉举报渠道，发挥专业机构、专家和家长等主体作用，加强社会监督。监管的出发点是促进有序健康发展，教育部将加强和相关职能部门的沟通协调，减少重复检查，避免对企业的正常运营造成不必要的干扰。（来源：中华人民共和国教育部）

- **教育部等八部门印发《关于引导规范教育移动互联网应用有序健康发展的意见》**
- **全文：**http://www.moe.gov.cn/srcsite/A16/moe_784/201908/t20190829_396505.html

➢ 工信部公开征求对《工业大数据发展指导意见（征求意见稿）》的意见

2019 年 9 月 4 日，工信部发布了《工业大数据发展指导意见(征求意见稿)》(下称《征求意见稿》)，提出到 2025 年，基本建成工业大数据资源体系、融合体系、产业体系和治理体系，并设置了建成国家工业互联网大数据中心、培育 3-5 个达到国际先进水平的工业大数据解决方案供应商、创建一批推动工业大数据集聚发展的国家新型工业化产业示范基地等具

体目标。

今年全国两会，“工业互联网”首度写入政府工作报告。工业互联网正成为诸如腾讯等互联网巨头重点发力的领域，也是新经济的蓝海，而工业大数据则是工业互联网的“粮食”。在业内人士看来，工信部《征求意见稿》的出台正当其时，有助于解决工业大数据行业当前存在的“数据孤岛”、基础设施缺失等一系列问题。

5 年建成工业大数据体系

工业大数据是制造业数字化、网络化、智能化发展的基础性战略资源，正在对制造业生产方式、运行模式、生态体系产生重大而深远的影响。推动工业大数据发展，是促进工业经济向数据驱动型创新体系和发展模式转变的关键。

对于大数据产业发展目标，《征求意见稿》提出，到 2025 年，基本建成工业大数据资源体系、融合体系、产业体系和治理体系，形成从数据集聚共享、数据技术产品、数据融合应用到数据治理的闭环发展格局，使工业大数据成为支持工业高质量发展的关键要素和创新引擎。

《征求意见稿》还设置了一系列“具体目标”。在数据资源高效汇聚方面，将建成国家工业互联网大数据中心、制造强国产业基础大数据平台等国家级基础工业数据资源平台。在融合应用繁荣发展层面，将培育 3-5 个达到国际先进水平的工业大数据解决方案供应商。在增强技术实力方面，将形成一批技术先进、可满足重大应用需求的大数据软硬件产品，创建一批推动工业大数据集聚发展的国家新型工业化产业示范基地等。

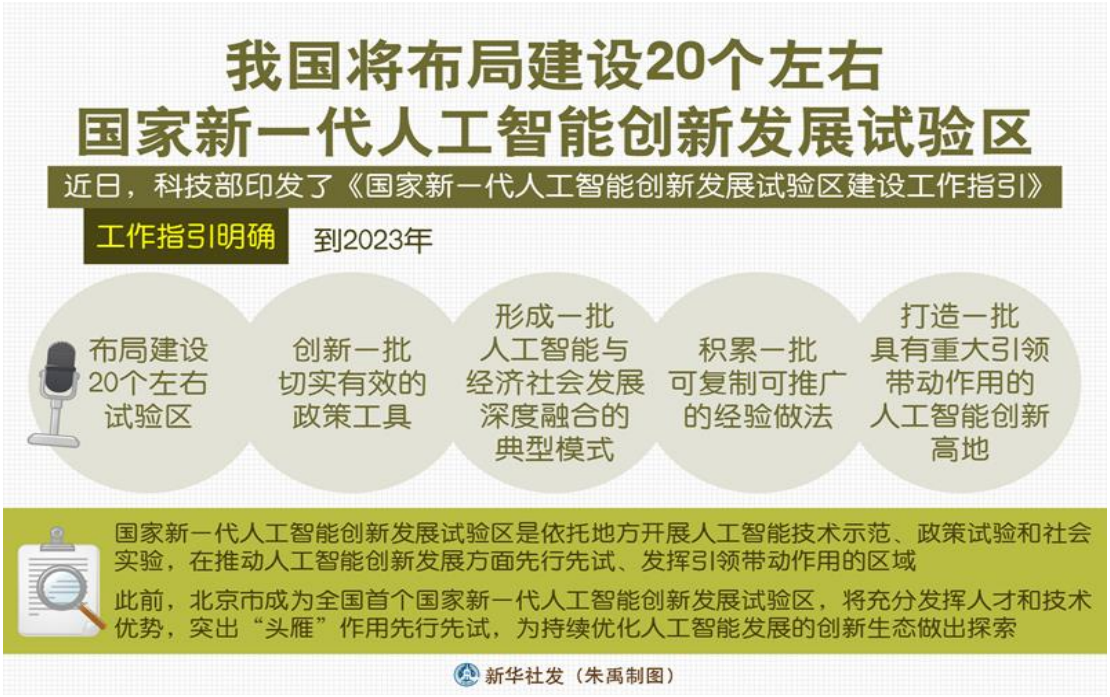
另外，为完善工业大数据治理体系，《征求意见稿》提出完善工业大数据法规标准、推动工业大数据分类分级管理等强化发展保障。比如，组织开展工业大数据分类分级、全生命周期处理、数据管理等标准的研制工作，促进国家标准、行业标准和团体标准等各类标准之间的衔接配套；制定《工业数据分类分级指南》，实现数据的差异化管理。（来源：中华人民共和国工业和信息化部）

- **《工业大数据发展指导意见（征求意见稿）》的意见**
- **全文：**http://www.miit.gov.cn/n1278117/n1648113/c7393004/content.html

➢ 科技部印发《国家新一代人工智能创新发展试验区建设工作指引》通知

2019 年 9 月 5 日，科技部印发《国家新一代人工智能创新发展试验区建设工作指引》

（以下简称“《指引》”）的通知。



《指引》提出，试验区建设以直辖市、副省级城市、地级市等为主，拟申请建设试验区的城市应具备以下条件：

一、科教资源丰富：应拥有设立人工智能学院或研究院的高校，拥有人工智能基础研究或关键技术领域的高水平研发机构，拥有一批高水平的人工智能创新团队。二、产业基础较好：原则上应是国家自主创新示范区或国家高新区所在城市，并已明确将发展人工智能作为重点产业方向，人工智能核心产业规模超过 50 亿元，人工智能相关产业规模超过 200 亿元。

三、基础设施健全：数据资源丰富，拥有相关的数据平台、大数据中心和云计算中心，移动通信、物联网、工业互联网等网络基础设施较为完善。优先支持已布局国家新一代人工智能开放创新平台的城市。

四、支持措施明确：地方政府对人工智能发展高度重视，已出台人工智能发展规划或实施意见。地方对人工智能有明确资金和政策支持，设立人工智能专项资金，政府相关部门设有专门人工智能推进机制或机构。

此外，《指引》提出，对于人工智能产业优势明显、智能化基础设施健全、应用场景特色突出、具有较强技术研发和成果转化能力的部分县域，也可申请建设国家新一代人工智能创新发展试验区。（来源：科技部）

- **科技部关于印发《国家新一代人工智能创新发展试验区建设工作指引》的通知全文：**
- http://www.most.gov.cn/mostinfo/xinxifenlei/fgzc/gfxwj/gfxwj2019/201909/t20190905_148663.htm

五、本期重要漏洞实例

➢ 关于 Microsoft 远程桌面服务存在远程代码执行漏洞的安全公告

发布日期：2019-09-07
更新日期：2019-09-07
受影响系统：
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems ServicePack 1
Windows Server 2008 for 32-bit SystemsService Pack 2
Windows Server 2008 for 32-bit SystemsService Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-BasedSystems Service Pack 2
Windows Server 2008 for x64-based SystemsService Pack 2
Windows Server 2008 for x64-based SystemsService Pack 2 (Server Core installation)
Windows Server 2008 R2 for Itanium-BasedSystems Service Pack 1
Windows Server 2008 R2 for x64-basedSystems Service Pack 1
Windows Server 2008 R2 for x64-basedSystems Service Pack 1 (Server Core installation)
Windows XP SP3 x86
Windows XP SP2 x64
Windows XP Embedded SP3 x86
Windows Server 2003 SP2 x86
Windows Server 2003 SP2 x64
描述：

2019 年 5 月 15 日，国家信息安全漏洞共享平台（CNVD）收录了 Microsoft 远程桌面服务远程代码执行漏洞（CNVD-2019-14264，对应 CVE-2019-0708）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。近日，漏洞利用代码（EXP）已公开，引起了安全研究人员的广泛关注，微软公司官方补丁已发布。
Microsoft Windows 是美国微软公司发布的视窗操作系统。远程桌面连接是微软从 Windows 2000 Server 开始提供的功能组件。
2019 年 5 月 14 日，微软发布了月度安全更新补丁，修复了远程桌面协议（RDP）远程代码执行漏洞。未经身份验证的攻击者利用该漏洞，向目标 Windows 主机发送恶意构造请求，可以在目标系统上执行任意代码。由于该漏洞存在于 RDP 协议的预身份验证阶段，因此漏洞利用无需进行用户交互操作， 存在被不法分子利用进行蠕虫攻击的可能。
近日，Metasploit 发布了该漏洞的利用模块，GitHub 网站上也公开了该漏洞的利用代码，引起了安全研究人员的广泛关注，存在被不法分子利用进行蠕虫传播的可能。根据奇安信 CERT 团队报送和 CNVD 秘书处验证结果显示，该漏洞利用仅对 Windows 7 SP1 x64 与 Windows 2008 R2 x64（非系统默认配置）系统版本有效，在虚拟机环境下复现成功。CNVD 对该漏洞的综合评级为“高危”。
<*来源：CNVD
链接：https://www.cnvd.org.cn/webinfo/show/5195
建议：

厂商补丁：

微软官方已于今年 5 月发布补丁修复此漏洞，CNVD 建议用户立即安装安全补丁：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/
另可采取下列临时防护措施：
1、禁用远程桌面服务。
2、通过主机防火墙对远程桌面服务端口进行阻断（默认为 TCP 3389）。
3、启用网络级认证（NLA），此方案适用于 Windows 7、Windows Server 2008 和 Windows Server 2008 R2。启用 NLA 后，攻击者首先需要使用目标系统上的有效帐户对远程桌面服务进行身份验证，然后才能利用此漏洞。
附：参考链接：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
https://msrc-blog.microsoft.com/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/
https://github.com/rapid7/metasploit-framework/pull/12283?from=timeline&isappinstalled=0

➢ WordPress photo-gallery 插件跨站脚本执行漏洞

发布日期：2019-09-06
更新日期：2019-09-10
受影响系统：
WordPress photo-gallery < 1.5.35
描述：

CVE(CAN) ID: CVE-2019-16117
WordPress 是一套使用 PHP 语言开发的博客平台。photo-gallery 是使用在其中的一个图片库插件。WordPress photo-gallery 插件 1.5.35 之前版本，在实现中存在跨站脚本漏洞。该漏洞源于 admin/models/Galleries.php 缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。
<*来源：vendor
建议：

厂商补丁：
WordPress
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://wordpress.org/plugins/photo-gallery/#developers
https://plugins.trac.wordpress.org/changeset/2150912/photo-gallery/trunk/admin/models/Galleries.php?old=2135029&old_path=photo-gallery%2Ftrunk%2Fadmin%2Fmodels%2FGalleries.php

➢ D-link DIR-806 代码注入漏洞

发布日期：2019-09-06
更新日期：2019-09-10
受影响系统：
D-Link DIR-806
描述：

CVE(CAN) ID: CVE-2019-10891
D-Link DIR-806 是一款无线路由器。
D-link DIR-806 设备在实现中存在代码注入漏洞，远程攻击者利用此漏洞可执行任意 shell 命令。
<*来源：vendor
建议：

厂商补丁：
D-Link
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://github.com/Kirin-say/Vulnerabilities/blob/master/DIR-806_Code_Injection.md

➢ Cisco Webex Teams 日志功能命令执行漏洞

发布日期：2019-09-04
更新日期：2019-09-06
受影响系统：
Cisco Webex Teams < 3.0.12427.0
描述：

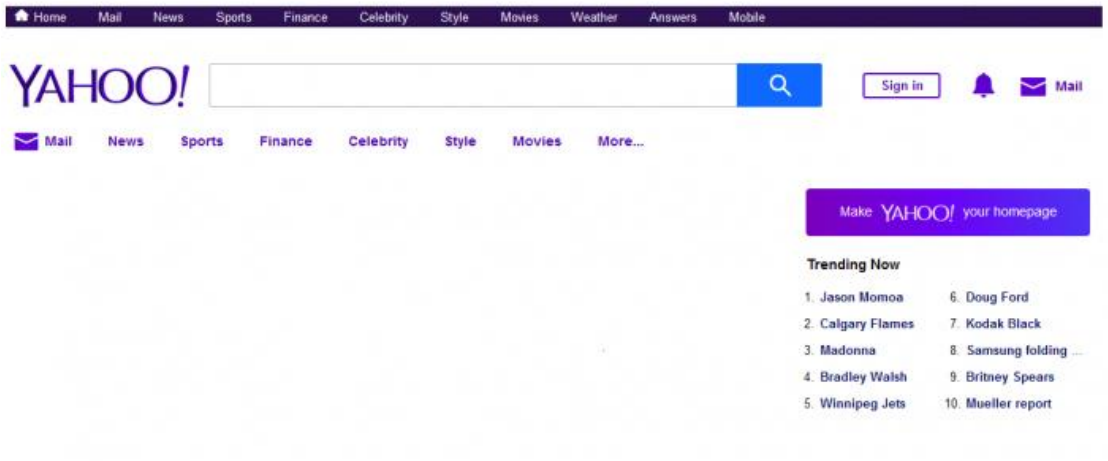
CVE(CAN) ID: CVE-2019-1939
Cisco Webex Teams 是实现持续性团队协作的应用。
Cisco Webex Teams client for Windows 在软件日志功能上没有正确的限制，存在安全漏洞，攻击者诱使用户浏览恶意网站，成功后可修改文件并执行任意命令。
<*来源：Chew Keong TAN （chewkeong@security.org.sg）
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-webex-teams
建议：

厂商补丁：
Cisco 已经为此发布了一个安全公告（cisco-sa-20190904-webex-teams）以及相应补丁：
cisco-sa-20190904-webex-teams：Cisco Webex Teams Logging Feature Command Execution Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-webex-teams

六、本期网络安全事件

➢ 雅虎发生全球宕机：邮箱、搜索等服务都无法正常使用

2019 年 9 月 5 日，据外媒 softpeia 最新报道，Yahoo.com 及其他服务在不久前下线，致使全球用户无法登录或连接到期在线门户网站。截止发稿前还没有关于此次宕机的详细信息。 尽管雅虎公司对与此次故障时间有关的所有事情都守口如瓶，但 DownDetector.com 等服务表明，美国旧金山、洛杉矶、达拉斯、西雅图和纽约都受到了影响。



另外，加拿大部分地区也遇到了无法连接 Yahoo 的问题。

至于在欧洲地区，来自法国、希腊和西班牙的大多数用户无法使用雅虎服务，来自意大利、英国和荷兰的许多用户也遇到了同样的情况。

在大多数情况下，Yahoo 服务根本都无法加载，虽然有些人声称他们成功进入了登录页面但之后却看不到任何内容。图像服务器似乎也没有正常使用。

而一些比较幸运的用户还可以进入他们的账户，但整个加载过程需要 5 分钟。主页的情况也是如此，不同地区表现则有所不同。（来源：softpeia）

➢ 谷歌同意为非法收集儿童信息支付 1.7 亿美金的罚款

2019 年 9 月 4 日，美国联邦贸易委员会（FTC）在其官网发布，谷歌旗下视频分享网站

YouTube 因非法收集和分享儿童个人信息被罚款 1.7 美元。其中，FTC 对谷歌罚款 1.36 亿美元，剩余 3400 万美元谷歌需向纽约州支付以了结类似指控。

据了解，这是自 1998 年颁布《儿童在线隐私保护 (Children's Online Privacy Protection Act，COPPA)以来，FTC 在儿童隐私案件中开出的最大民事处罚。

去年 4 月，20 多家保护机构、消费者和隐私权益组织组成的联盟向 FTC 投诉 YouTube 非法收集儿童数据。该联盟指控称，YouTube 收集大量 13 岁以下儿童用户的数据，包括电话号码和地理位置等信息，然后追踪他们在许多网站的浏览习惯，并在没有获得许可的前提下，利用这些信息提供精准广告服务。

根据 COPPA 规定，在收集、使用和披露 13 岁以下儿童的任何个人信息前须直接通知其父母，并取得父母“可验证的同意”（verifiable parent consent）。

FTC 和纽约州司法部表示，YouTube 未经父母同意，通过跟踪儿童频道观众网络浏览的识别码（cookie）向用户提供有针对性的广告，并从中赚取了数百万美元。

“YouTube 向潜在的企业客户推销自己是儿童最喜欢的视频网站。但在涉及到遵守保护儿童隐私的法律时，YouTube 却拒绝承认平台的部分内容是明确针对儿童的”，FTC 主席 Joe Simons 说。

据了解，FTC 以 3 票赞成、2 票反对的结果通过了和谷歌的和解协议，并将其提交给了美国司法部。除了罚款之外，该和解协议还要求 YouTube 修改其儿童内容的处理流程，以便其能够确保其遵守《儿童在线隐私保护法》。此外，和解协议还要求他们在收集儿童的个人信息之前，提供关于其数据收集做法的通知，并获得父母的同意。

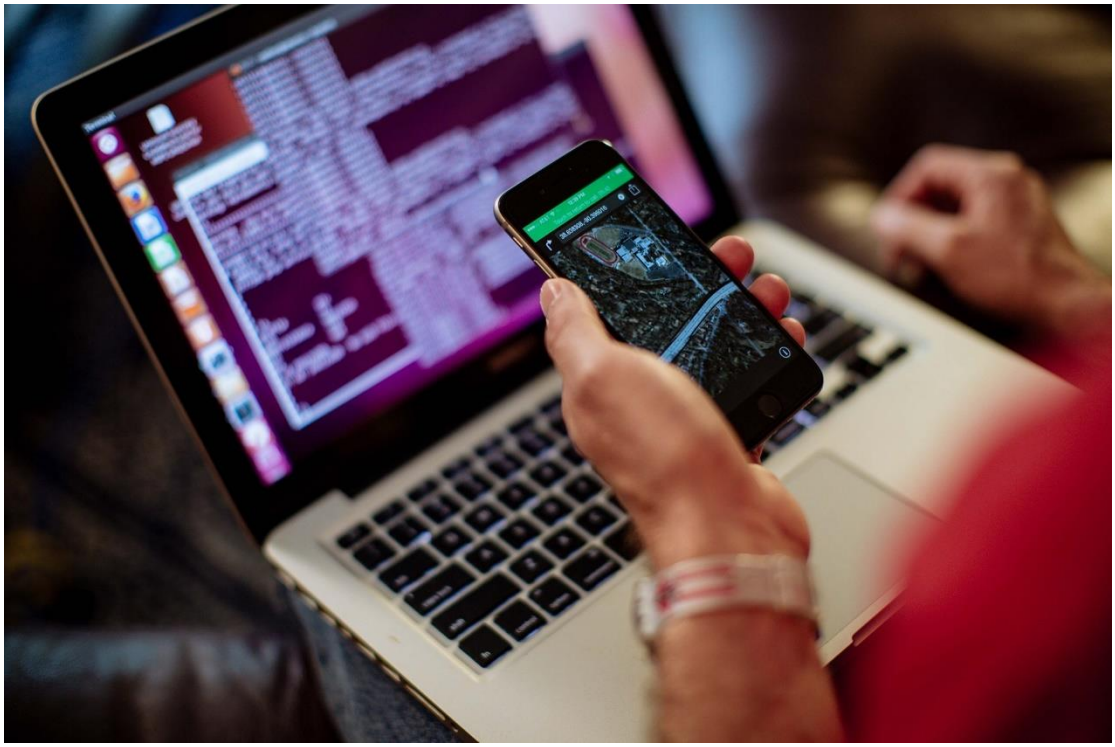
YouTube 首席执行官 Susan Wojcicki 表示：“不管用户年龄多大，我们会把任何在 YouTube 上观看儿童内容的用户数据视为是来自儿童的数据。这意味着我们将限制儿童视频的数据收集和使用，只会在支持服务运营所需范围内使用和收集数据。我们也将完全停止在这些内容

上投放个性化广告。”

事实上，在达成和解协议之前，谷歌已经推出了 YouTubeKids。谷歌表示，建立该网站“是为了给孩子创造一个更安全的环境，让他们探索自己的兴趣和好奇心，同时给父母提供工具，让他们为孩子定制体验。”家长可以从三个不同的年龄组中选择适合自己孩子的年龄组——学前班、5-7 岁和 8-12 岁。（来源：腾讯科技）

➢ 16 岁少年化身黑客利用系统漏洞盗取公司 80 余万被判 3 年 6 个月

2019 年 9 月 6 日，检察日报报道：2002 年,王某某出生于黑龙江。年幼的时候父母就离异了,父亲一直在外打工,他是由奶奶和姑姑抚养长大的。据姑姑介绍,王某某平时在家时很听话,学习成绩也很好,从不用家人操心。“每天放学后都直接回家,不喜欢出门,也不喜欢去娱乐场所,休息时更喜欢在家里自学计算机。”



因家里生活拮据 他利用掌握的技术盗取钱财

实际上,出于对计算机的热爱,王某某自初二起便开始买书自学计算机知识,并通过给一些公司编程、找漏洞获取酬劳,一笔能赚三四千。在赚钱的同时,王某某也在网络上结交了很多好朋友,平时在家里少言寡语的他在网络里更有活力,更喜欢和网友倾诉真实的内心想法。他说,在网上聊天很自由,没有束缚感,也不会感觉到别人对他有意见。

渐渐地,王某某对计算机设备的需求越来越多,他希望用更好的设备与朋友一起编程。但是,他知道家里生活拮据,就没有开口向家里要钱。为了能得到更好的主机、服务器等物,他开始利用自己擅长的技能来满足需求。有一次,王某某在测试软件时侵入某公司网站,抱着试一试的心态转了第一笔钱,然而他的行为并没有被发现,于是逐渐产生了侥幸心理,为之后的犯罪埋下了伏笔。在他看来,以他的技术,他的盗取行为是不会被发现的。

利用系统漏洞获取控制权 先后分 15 次提现 80 余万

2017 年 8 月 1 日开始,身在黑龙江某小区的王某某利用 Windows 系统漏洞攻击了北京某计算机服务系统公司旗下的游戏点卡销售平台,并获得了其平台的最高控制权,篡改商家数据信息并重置密码,在未进行任何交易的情况下,修改平台账户余额并提现到自己的财付通和支付宝账户内。在不到一年的时间内,王某某先后通过这种方式分 15 次提现,共计提现 81.6 万余元。据王某某交代,盗取的钱款除了借给朋友外,主要用于购买服务器等计算机设备和吃喝玩乐。

2018 年底,北京市海淀区检察院对涉嫌盗窃罪的未成年犯罪嫌疑人王某某依法批准逮捕。此后,海淀区检察院以王某某犯盗窃罪向北京市海淀区法院提起公诉。

其窃取行为构成盗窃罪被判有期徒刑三年六个月

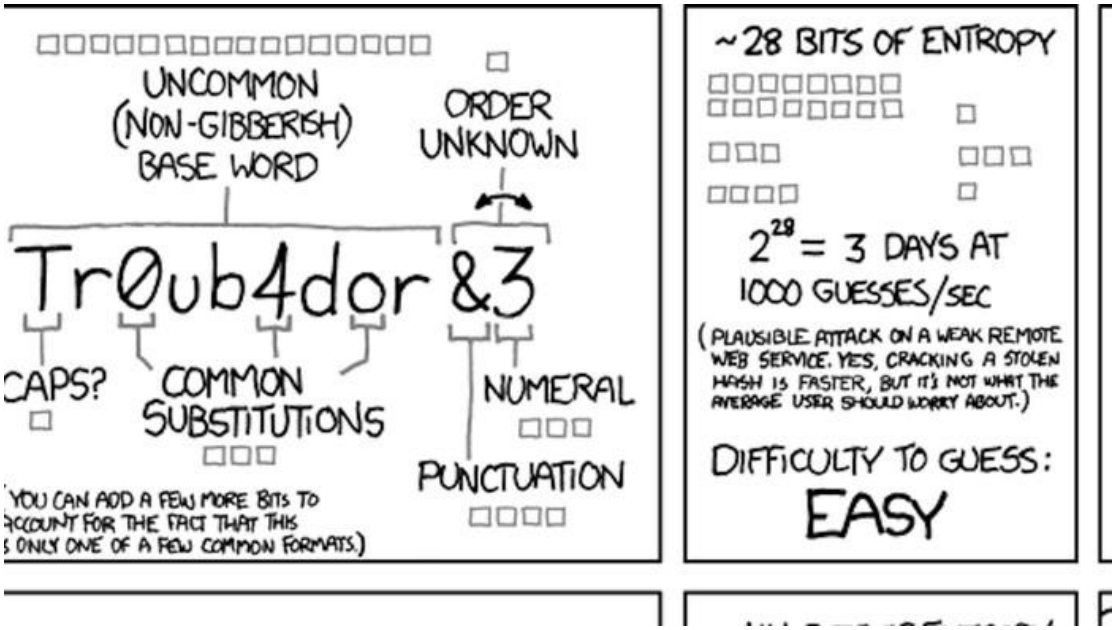
2019 年 6 月,北京市海淀区法院对此案作出了审判。海淀区法院经审理认为,王某某以非法占有为目的,通过篡改被害单位计算机系统后台信息的方式,秘密窃取他人钱款,数额特别巨大,其行为已构成盗窃罪。

王某某犯罪时不满十八周岁,系未成年人犯罪;到案后能如实供述主要犯罪事实,认罪态度较好;且其父母在案发后积极与被害单位协商,主动退还 50 万元,取得被害单位的谅解;结合王某某的一贯表现,海淀区法院依法对其减轻处罚。依照《中国人民共和国刑法》规定,判处被告人王某某有期徒刑三年六个月,共处罚金人民币三十万元。

检察官提醒：北京市海淀区检察院的承办检察官王敬敬表示,网络的背后,是风景还是深渊,就在一“键”之间。伴随着计算机网络在社会各领域中的广泛应用,网络犯罪也随之滋生,并日益演变成为危害当今社会秩序的主要犯罪行为之一。网络犯罪是以网络为犯罪工具或以网络为犯罪对象实施危害网络信息系统安全的犯罪行为。但是,网络虚拟世界不是虚幻的,更不是虚假的,它是现实社会在网络上的延伸,网络是社会的一部分,不会也不能有超出法律规定的绝对自由。（来源：检察日报正义网）

➢ 人气网络漫画 XKCD 论坛遭网络攻击：大量用户数据被盗

2019 年 9 月 4 日，据外媒报道，黑客攻击了人气网络漫画网站 XKCD 的论坛并从中窃取了约 56 万个用户名、电子邮件和 IP 地址以及散列密码。XKCD 在周末公开了这次攻击，此前，负责数据漏洞通知网站 Have I Been Pwned 维护工作的安全研究员 Troy Hunt 向该网站发出了警告。现在，这个论坛已经下线。



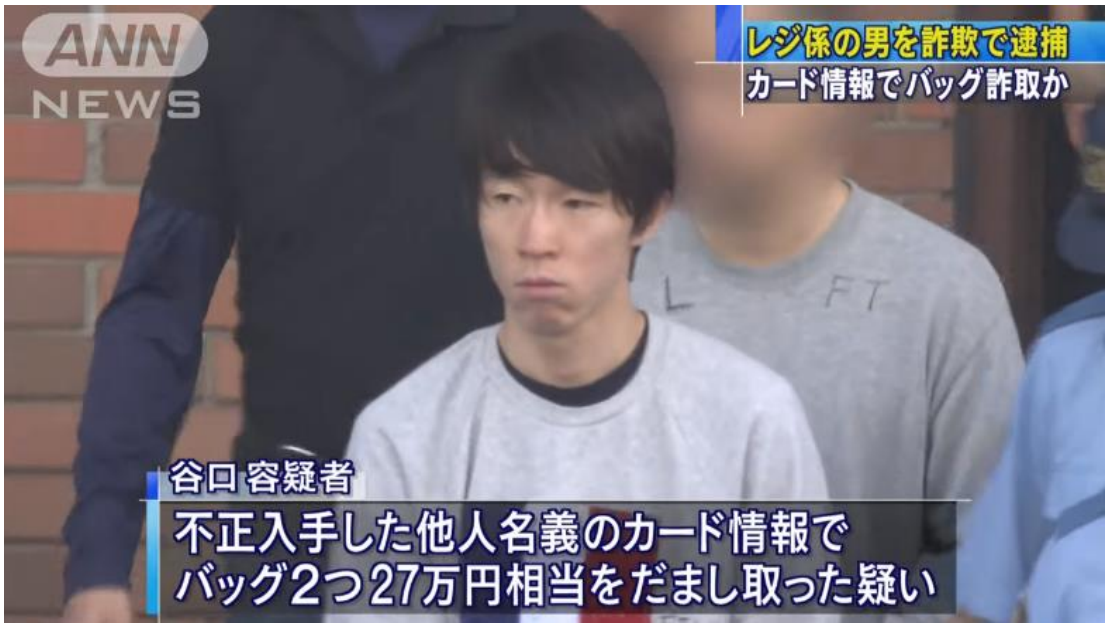
论坛方面表示，等到他们能够检查漏洞并确保论坛已经安全之后才会重新上线这个论坛。“如果你是 echochamber.me/xkcd 用户，那么你应当立即更改你使用了同一个或类似密码的另一个账号的密码。”

XKCD 是 Randall Munroe 创作的流行网络漫画，其已经有 14 年的历史、主要关注科技、科学和互联网文化。Munroe 还以其现在的标志性简笔人物画风格出过几本书，包括《How To》、 《Thing Explainer》、《What If》。

Hunt 表示，这些数据由白帽子公安全研究员 Adam Davies 发现。（来源：cnBeta）

➢ 日本收银员"过目不忘" 疯狂盗刷顾客 1300 张信用卡

2019 年 9 月 9 日，好莱坞明星莱昂纳多在电影《猫鼠游戏》(英文名：Catch Me If You Can)里饰演一位天才诈欺犯，据介绍该故事是根据真人真事改编。近日，日本也传出一起令人称奇的犯罪事件，一位东京大卖场内的收银员，利用“过目不忘”的能力盗刷了顾客 1300 多张信用卡。



据日本朝日电视台(ANN)9 月 7 日报道，34 岁的谷口裕介是东京江东区一家大卖场内的收银员，近日被警方以盗刷信用卡的罪名逮捕。嫌犯之所以能够顺利盗刷信用卡，凭借的是拥有超强视觉记忆力，当顾客拿出信用卡结帐时，谷口裕介便利用帮客人刷卡的短时间内，暗自将卡片的号码、有效日期、安全码等信息全数牢记在心。

警方在谷口裕介的房间内找到一本记事本，上面记载了 1300 张顾客的信用卡信息，谷口裕介便是凭着这些信息，在网上购物满足生活上的开销，更从海外邮购网站买商品，并用二手价卖出换取现金。目前，警方以非法盗刷信用卡罪名将他逮捕，直到东窗事发他的行为才被迫停止。

网友对谷口裕介的做法表示难以置信，有人认为谷口裕介是浪费天赋，也有人对于其记忆力表示好奇。网友表示：“我一张卡号都记不住这个厉害了。”更多网友认为：“这个只做收银员太浪费了吧。”“有这能力为什么不去考好一点的工作啊。”“才能用错地方。”（来源：海外网）

➢ 国内首例微信支付赎金勒索病毒案一审宣判 “95 后”黑客获刑六年

2019 年 9 月 3 日，利用电脑感染病毒后弹出微信支付二维码，用户被要求支付 110 元才能获得解密密匙，该病毒共导致 2 万多台电脑“中招”。东莞市第三人民法院对国内首例微信支付赎金的勒索病毒案作出一审判决，以犯破坏计算机信息系统罪，判处制作该病毒的“95 后”男子罗某有期徒刑六年六个月。

2018 年 12 月 1 日，多名用户称其电脑感染一款需要使用手机扫描微信支付二维码支付 110 元赎金的病毒。据悉，这是国内首次出现要求使用微信支付的勒索病毒，该病毒采用“供应链感染”方式通过论坛传播，同时还窃取用户淘宝、支付宝、QQ 等账号密码。公安机关于 2018 年 12 月 5 日将制作这款病毒的黑客罗某抓获，并在其住处查获电脑、手机等作案工具。

据了解，罗某是一名高中辍学的“95 后”，虽文化程度不高，但对计算机兴趣浓厚。罗某于 2018 年 1 月在东莞东坑镇一间出租屋研发“cheat”木马病毒，预谋盗取他人支付宝等网络账号和密码。2018 年 11 月，他租用河南郑州一家网络公司服务器，将病毒植入一个软件模块并在论坛发布，病毒会对下载该软件的计算机进行感染。该病毒运行后，对计算机的文件进行加密，并弹出附有微信收款二维码的勒索窗口，向每台感染病毒的计算机用户敲诈勒索 110 元，共收款 37 笔，其中一笔 30 元，非法所得 3990 元。

经司法鉴定，该病毒程序会对用户主机中存储的数据进行加密，为未授权地修改、干扰，故为破坏性程序，共感染电脑主机数量为 27939 台；该病毒具有通过监控用户键鼠操作来获取用户网络账号、密码信息的功能，共记录键盘鼠标操作记录有 21546 条。检察机关认为，被告人罗某违反国家规定，故意制造、传播计算机病毒等破坏性程序，影响计算机系统正常运行，应当以破坏计算机信息系统罪追究其刑事责任。

法院认为，罗某故意制造、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果特别严重，其行为已构成破坏计算机信息系统罪，期间还进行盗窃、敲诈勒索，同时也触犯敲诈勒索罪、盗窃罪。根据被告人罗某的犯罪情节及悔罪表现，法院判处其有期徒刑六年六个月。（来源：东莞时间网）

信息安全意识产品年服务

021-33663299