国盟信息安全通报

2019 年 12 月 23 日第 208 期

国盟信息安全通报

（第 208 期）

国际信息安全学习联盟

2019 年 12 月 23 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 327 个，其中高危漏洞 133 个、中危漏洞 172 个、低危漏洞 22 个。漏洞平均分值为 6.15。本周收录的漏洞中，涉及 0day 漏洞 120 个（占 37%），其中互联网上出现“WordPress CSS Hero 插件跨站脚本漏洞、Intelbras WRN 150 跨站请求伪造漏洞”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 2695 个，与上周（2338 个）环比增长 15%。

主要内容

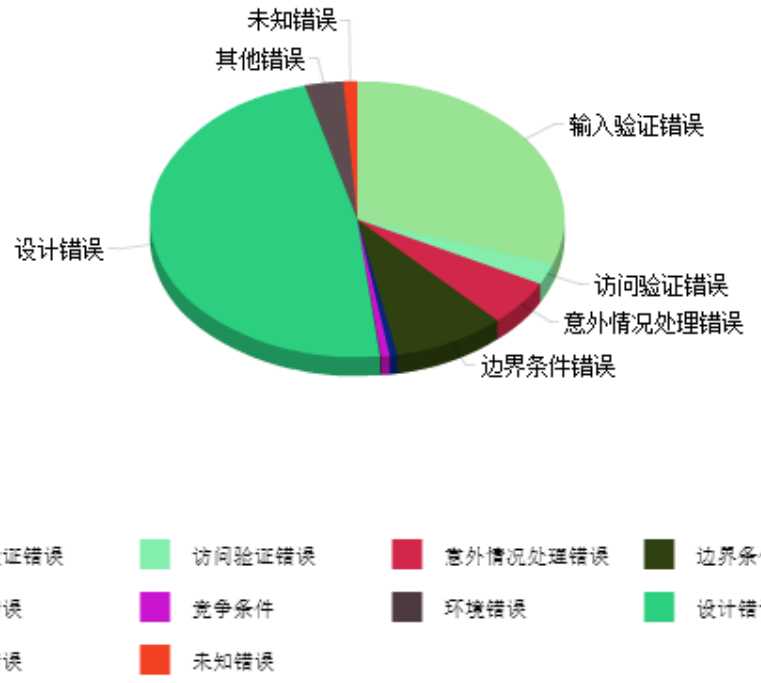
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

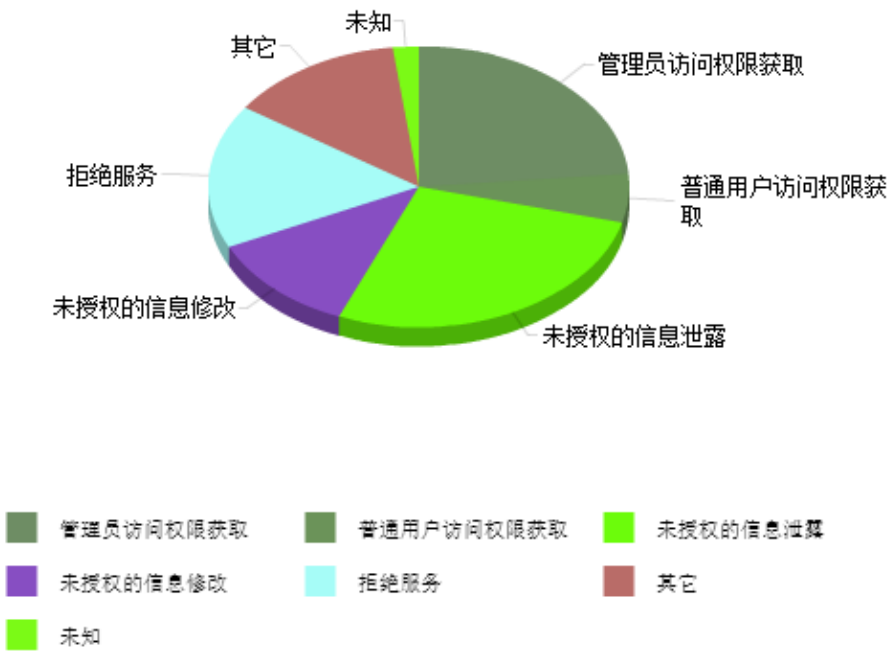
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 327 个，其中高危漏洞 133 个、中危漏洞 172 个、低危漏洞 22 个。漏洞平均分值为 6.15。本周收录的漏洞中，涉及 0day 漏洞 120 个（占 37%），其中互联网上出现“WordPress CSS Hero 插件跨站脚本漏洞、Intelbras WRN 150 跨站请求伪造漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2695 个，与上周（2338 个）环比增长 15%。

二、安全漏洞增长数量及种类分布情况

➢ 漏洞产生原因（2019 年 12 月 09 日—2019 年 12 月 23）



➢ 漏洞引发的威胁（2019 年 12 月 09 日—2019 年 12 月 23）



➢ 漏洞影响对象类型（2019 年 12 月 09 日—2019 年 12 月 23）

三、安全产业动态

➢ 以四中全会精神为指引 推进新时代网信工作迈上新台阶

【编者按】近期，全国网信系统学习宣传贯彻党的十九届四中全会精神宣讲活动在各地取得了积极反响。为结合网信工作实际进一步深入学习领会四中全会精神，中国网信网对参与宣讲的部分专家学者进行专访，从多个角度解读四中全会精神，助您学懂弄通，学以致用。

十九届四中全会是中国处于中华民族伟大复兴关键时刻召开的一次具有开创性、里程碑意义的会议，全会审议通过的《决定》回答了我国国家制度和国家治理体系要“坚持和巩固什么、完善和发展什么”这个重大问题，为新时期做好网信事业提供了科学指南和根本遵循，是做好网信工作的总纲领、总规划，是确保网信事业沿着正确政治方向前进的基本保障。

网信系统进一步推动四中全会精神的贯彻落实工作，需要全面准确把握党的十九届四中全会精神的丰富内涵和核心要义，准确把握坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化的总体要求、总体目标和重点任务。要推出更多具有网络特点、适应网民需求的宣传内容，形成全方位、多层次、多声部的传播矩阵，在网上唱响学习贯彻全会精神的“大合唱”。

以全会精神作为新时代网信工作的指引

全会《决定》围绕“坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力

现代化”这一主题对一系列问题所做出的重大部署，都与网信工作密切相关，都是新时代做好网信工作的指引，以下几个方面与网信工作的联系更为直接，了解这些要求，对做好新时代网信工作至关重要。

在涉及公共管理和构建公共服务体系方面，有许多内容直接涉及网信工作，包括创新互联网时代群众工作机制；用互联网、大数据等完善公共服务体系，推进数字政府建设、推进数据有序共享和保护个人信息；把数据作为生产要素参与市场评价和报酬确定；优化经济治理基础数据库等。

有些部分没有直接提到网信领域的具体要求，但主要针对的是网信工作。《决定》提到的外商投资国家安全审查、反垄断审查、国家技术安全清单管理、不可靠实体清单等制度构建的要求，都与网信工作，尤其是做好网络安全工作密切相关，这些制度是确保网络安全的重要抓手，也是落实网络安全工作的前置性要求。

《决定》还要求健全全面贯彻落实习近平新时代中国特色社会主义思想，健全用党的创新理论武装全党、教育人民工作体系，完善党委（党组）理论学习中心组等各层级学习制度，建设和用好网络学习平台。《决定》也提到了用互联网、人工智能促进教育的作用和重要性，以及在推进“一带一路”建设过程中，要推动解决全球发展失衡数字鸿沟等问题。

在牢牢抓住网络意识形态阵地方面，《决定》着墨最多，要求也更为全面。具体要求包括：完善坚持正确导向的舆论引导工作机制。坚持党管媒体原则，坚持团结稳定鼓劲、正面宣传为主，唱响主旋律、弘扬正能量。构建网上网下一体、内宣外宣联动的主流舆论格局，建立以内容建设为根本、先进技术为支撑、创新管理为保障的全媒体传播体系。改进和创新正面宣传，完善舆论监督制度，健全重大舆情和突发事件舆论引导机制。建立健全网络综合治理体系，加强和创新互联网内容建设，落实互联网企业信息管理主体责任，全面提高网络治理能力，营造清朗的网络空间。

协调安全和发展 抓牢信息革命的历史机遇

网信工作牵一发而动全身，有很强的系统性和全局性。做好网络安全和信息化工作，关系到我们能不能利用好这次信息革命给我们带来的千载难逢的机遇，通过全面提升管理水平，实现制度建设方面的重大推进，为逐步实现两个一百年奋斗目标，实现中华民族伟大复兴的中国梦打下良好基础。

习近平总书记强调，没有网络安全就没有国家安全。可见网络安全在国家安全中的重要地位和作用。如果不能解决好网络安全问题，国家安全、人民生命财产安全和社会稳定发展、经济增长方式的转型等，都可能面临这样或那样的风险，都有中断我国现代化进程的可能。

因此，必须通过健全网络安全制度，落实网络安全监管措施，不断突破影响网络安全的核心技术，尤其是具有基础、核心和全局性的技术，为中国特色社会主义制度建设提供稳定的条件，打下扎实的基础。

习近平总书记指出，没有信息化就没有现代化。信息化是现代化的内在动力，是现代化的翅膀。没有信息化或信息化不充分、不彻底，现代化就是空话，就是空中楼阁。也可以说，信息化是现代化的前提。

无论是治理体系还是治理能力的现代化，都需要充分利用最先进的信息技术，都需要利用大数据、人工智能等新技术提升各项工作的科学性，增加各项方案的合理性，避免社会发展过程中随时可能遇到的不确定性和风险，从容应对和驾驭现代化过程中遇到的各种困难和风险。

世界正处于引发社会生产方式产生革命性巨变的信息革命的前夜，中国为这一变革做了较世界上其他国家更为成功、更为彻底且更为充分的准备，5G、大数据、人工智能等技术的发展走到了世界前列，我们一定要充分利用好这些有利条件，协调好安全与发展的关系，抓住这一历史机遇，使中国特色社会主义焕发出更加强大的生机和活力。

坚持党的领导对网信工作意义重大

网信机构、组织和企业的发展，必须以党的政治建设为统领、必须坚持党的领导。这是由中国特色社会主义制度的本质特征决定的，也是对网信事业、组织和企业健康发展提出的内在要求。

中国特色社会主义制度的最本质特征，就是坚持党的领导，用党的纲领、用党的信念和党的方针政策统领指导各项事业。作为我国各项事业重要组成部分的网信事业、组织和企业的各项工作，也必须在党的领导下进行。

在网信机构、组织和企业坚持以党的政治建设为统领、坚持党的领导，有利于将网信事业置于中国共产党所统揽的伟大斗争、伟大事业、伟大梦想当中，使网信事业能够在面对百年未有之大变局的情况下保持发展的动力、活力和正确的发展方向，使我国网信事业成为党的事业和人民的事业的有机组成部分，在国家建设的过程中、在中国特色社会主义制度完善和发展的过程中、在国家治理体系和治理能力现代化的过程中，发挥更加稳定和重要的作用。

在网信机构、组织和企业坚持以党的政治建设为统领、坚持党的领导，也是网信事业快速发展提出的内在要求。网络安全事关国家安全、事关我国现代化实现的程度和质量，一方面与两个一百年奋斗目标的实现、与中国梦的实现同步关联，同时又具有自身特点，网信事业只有和党的领导保持同步性、共振性，以党的建设为统领，才能获得稳定而持久的精神动

力，才能与党的各项其他事业同步、同向发展，也才能将网信事业置于党的事业的宏大蓝图之中，不走偏、不掉链、不迷失。（来源：网信中国 作者：中国传媒大学人类命运共同体研究院 副院长、教授 王四新）

➢ 工信部：今年中国网络安全产业规模将超 600 亿元

2019 年 12 月 9 日，工信部网络安全管理局局长赵志国在 2019 年中国网络安全产业高峰论坛上称，“十三五”以来，我国网络安全产业保持高速增长，2019 年产业规模预计超过 600 亿元，年增长率超过 20%，明显高于国际 8%的平均增速，保持健康的发展态势。

网络安全产业投融资也更加活跃。工信部披露的数据显示，截至 2019 年 11 月底，公开融资方面，国内上市的网络安全企业达到了 23 家，创新孵化方面，有 100 多家创投机构在网络安全领域进行投资布局，汇集超过了 150 家创新创业的企业。

5G、大数据、云计算、工业互联网、人工智能、区块链等新兴技术在为我国经济社会发展注入强劲动力的同时，也带来了很多风险挑战和不确定因素。

工信部副部长陈肇雄在上述论坛上表示，工信部着力培育壮大网络安全产业生态，统筹推进北京、湖南等地建设国家网络安全产业园区，集聚发展效应初步显现，开展网络安全技术应用试点示范、工业互联网创新发展工程，带动投资超 160 亿元。

与此同时，网络安全产业的短板也日渐突出。“产业整体规模偏小，2018 年产业规模仅占全球 6%。”赵志国说，我国安全实力相对较弱，缺乏龙头企业；网络安全的核心元器件、核心设备和基础通用软件等关键核心技术缺乏；我国产业创新的能力不足，产业发展的环境也有待于进一步完善；企业和产品国际市场的认可度还不高，国际竞争力和输出的能力相对较弱。

陈肇雄强调，必须突破关键技术，掌握安全发展主动权。加强网络安全基础性、通用性、前瞻性技术创新研究，努力攻克基础技术，解决网络本质安全问题。打造良好产业生态。培育壮大若干网络安全龙头企业，鼓励带动一批中小企业，推动大中小企业融通发展。推动各行业各领域持续加大网络安全投入，加强供需对接、产融结合，促进网络安全产业更好满足各行业各领域需求。

为加快构建新兴融合领域安全保障体系，工信部会同九部门联合印发《加强工业互联网安全工作的指导意见》，构建协同推进、各司其责的安全工作体系，超前谋划 5G、车联网、人工智能等新兴技术领域安全风险应对。

各地政府也正在全面实施网络强国战略，努力构建与信息化发展水平相适应的网络安全产业体系和管理服务体系。比如，北京市将网络安全产业作为全市优先发展的高精尖产业方向，坚持创新驱动，坚持开放合作，积极营造网络安全产业发展良好的生态环境。（来源：工业和信息化部网站）

➢ 金融 App 信息保护受关注：测试 30 款有 17 款索取隐私权限

近日，100 款 App 整改通告中多家金融机构“上榜”，让金融机构的数据安全与个人信息保护问题引起了广泛关注。记者采访金融、安全行业多位圈内人士发现，随着移动支付的发展，越来越多的金融机构将借贷、支付场景转移到了线上，在这一过程中，许多银行遭遇到了新麻烦，包括如何达到国家规定的安全标准、如何对抗浸淫互联网圈已久的黑产攻击，以及如何让 App 既实现多项业务功能，还可在个人信息保护上合规。

12 月 10 日至 16 日，记者下载 30 款排名靠前的金融类 App 测试发现，金融 APP 超范围索取权限问题仍然存在。30 款 App 中有 17 款 App 索取了隐私权限，其中 13 款 App 索取了位置权限。“怎么判断 App 的权限‘越界’，我们之前也不了解。但所有银行自成立之初，就一直有风控部门在把关风险。只不过，在从线下支付到移动端支付的发展过程中，我们遇

到的风险形态已经发生了很大变化，金融机构在这方面的投入也逐年升高，内控、抵御黑产攻击、信息保护合规，很多地方需要注意。”某银行高管戴蒙（化名）告诉记者。

测试 30 款 App：17 款索取隐私权限，其中 13 款索取位置

金融 App 近期正遭遇又一轮监管。12 月初国家网络与信息安全通报中心发布通报指出，公安机关在开展 App 违法违规采集个人信息集中整治中，下架整改 100 款违法违规 App，其中光大银行、天津银行等金融类 App 上榜。

对此，一位不愿具名的接受整改 App 的高管对记者表示，“之前我们接到通知说我们的 App 存在泄露客户隐私的问题，具体问题包括隐私协议不规范和超范围收集，但目前已经整改完了。”

12 月 10 日至 16 日，记者在华为应用市场随机下载了 30 款排名靠前的金融类 App 测试

发现，若按照全国信息安全标准化技术委员会 2019 年 8 月 8 日发布的《信息安全技术 移动互联网应用（App）收集个人信息基本规范（草案）》规定的金融借贷类 App 必要权限范围，这 30 款 App 中有 25 款在首次打开时超范围申请了权限。如光大银行申请位置权限，好分期申请通讯录、位置，闪电借款申请位置，民贷天下申请录音、拍照权限等。这说明，金融 App 超范围索取权限问题仍然存在。不过记者注意到，即便拒绝上述权限索取要求，这些 App 仍可继续使用。

但需要注意的是，根据《信息安全技术 移动互联网应用（App）收集个人信息基本规范（草案）》规定，金融借贷类 App 为用户提供从金融机构进行个人消费贷款服务，包括授信、借款、还款与交易记录等功能（其中金融机构是指有放贷资质的银行、消费金融公司、小贷公司等在网络上提供借贷服务的机构）。金融借贷类 App 的必要权限只有存储权限一个，即除了存储权限，对其他任何权限的索取都涉嫌超限索权。

记者发现，许多金融类 App 除了收集必要的手机存储权限外，往往还会收集设备信息权限，如 360 借条、度小满理财等，而这也是导致众多金融类 App 涉嫌超限索权的原因。有熟悉隐私行业的专家表示，设备信息包含手机识别码，一些基本功能如认证登录等均需要手机识别码的支持，此外，该项权限在互联网广告领域也是用来追踪用户的重要标识，因此众多 App 都会收集该项权限。

根据上述《规范》，相机、通讯录、位置、麦克风、短信等权限属于“隐私权限”范畴。记者测试上述 30 款金融类 App 发现，30 款 App 中有 17 款 App 索取了隐私权限。其中位置权限被索取得最频繁，有 13 家 App 均索取了位置权限。

上述金融类 App 均在首页对隐私政策进行了弹窗公示，一些 App 则对索取权限的理由也进行了解释。如拉卡拉在首次安装打开后便弹窗表示其有可能索取定位、相机权限。其中索取定位权限的目的是用位置信息评估业务风险，而相机则用于身份确认。而招商银行则弹窗提示开启定位权限，目的是提高查询本地城市服务、附近优惠商户的准确性。好分期申请了通讯录与位置权限，其在首页弹窗对申请权限的行为作出解释称，“允许访问通讯录可以有效提升审核效率，允许访问位置可以提升好分期商城体验”。

对此，金融科技专栏作家、资深观察人士毕研广对记者表示，金融类 App 正常收集个人信息，以便于风险控制、门槛设立、投资者测评等是有必要的。比如个人办理贷款时，银行需要掌握个人基本的身份信息、财力状况等，至于读取相应通讯录信息、短信信息等则没有必要。

超限索权、黑产、“内鬼”，银行类 App 成风险“重灾区”

12 月 16 日，戴蒙对记者表示，其所在的银行曾遭遇监管机构的整改通告，原因是其索取了用户的通讯录权限与位置权限。戴蒙表示，索取通讯录权限仅是为了方便用户向好友转账，而位置权限则是告知线下网店的位置。他透露，监管部门并未全面禁止不允许索取上述权限，只是一定要在隐私协议里对索取权限的原因有所体现。

还有业内人士对记者表示，其实很多银行的 App 是找外包团队做的，“虽然在应用市场看到 App 的运营商是银行自己，但实际上做 App 的另有其人。而程序员如果在做 App 时‘抄了’其他 App 安装包的内容，就有可能导致权限索取的部分也一起‘抄’过来了，最后导致隐私不合规。”

根据中国信息通信研究院此前发布的《2019 金融行业移动 App 安全观测报告》，在具有典型代表性的 12 款下载量过亿的金融行业 App 中，多款 App 存在不同程度的超范围索取用户权限的情况，在隐私政策方面也存在多种违法违规行为，给用户个人隐私信息安全带来隐患。App 用户的个人隐私信息一旦泄露，将带来严重的后果，如骚扰电话、信息诈骗、恶意推销、网络情感诈骗等，会严重损害 App 用户的利益。

在不少安全专家看来，银行 App 里面包含了很多重要的客户数据，而权限索取则是获取客户数据的途径之一，因此不论是出于业务考虑还是无心之失，过多收集客户数据的同时，如果银行的风控系统不到位，客户信息也很容易被黑产或“内鬼”所窃取。

记者查阅黑猫投诉平台关于金融消费者的投诉情况发现，客户信息泄露成为了保险业的前三大“差评”之一，另外两个为违规销售和理赔难。

12 月 13 日，奇安信集团副总裁梁志勇在接受记者采访时表示，现在数据安全事件发生的频率越来越高，单个企业遭受的损失也越来越大。例如 2017 年美国的一家信用卡公司发生了 1.5 亿张信用卡信息泄露，给民众隐私和企业自身都带来了很大伤害。

“数据泄露的渠道包括外部黑产攻击以及内部威胁两种，其中内部威胁实际上是数据安全很重要的一个场景。例如一些机构有非常有价值的数据，内部人员一般都有合法的身份，但他们若出于利益或其他目的，就会违规地使用数据，这类事件在一些有重要数据的企业里较易发生。”梁志勇表示。

“金融机构汇聚了大量公民信息和交易数据，并且保障着社会生产秩序的有序进行。因此对于金融机构来说，首要的是保证数据不发生泄露，其次要保证金融服务的稳定性和持续性。网银、电子支付、手机银行也是普遍意义上金融机构易受到攻击的应用，主要风险包括：网络嗅探、拒绝服务、撞库等网络安全风险，数据防泄露、防篡改等数据安全风险以及内部数据窃取、恶意使用等业务风险。”12 月 16 日，腾讯安全云鼎实验室负责人董志强对记者

表示。

12 月 11 日，央行科技司司长李伟在 2019 年“中国金融科技全球峰会”上表示，前不久对金融类 App 开展标准测评和认证后，近期注意到几部委开展的对 App 风险的整治，其中银行类 App 是风险重灾区，所以将加快推进有关工作，切实防范化解风险。

“随着互联网金融新的发展，风险也有了新的变化和特征。2019 年的政府工作报告中，未曾提及互联网金融，却在金融领域提及 23 次‘风险’问题，可见，在新时期下，互联网金融的风险以及犯罪问题仍然是对互联网金融关注的重点。”中南财经政法大学法治发展与司法改革研究中心教授郭泽强表示。

监管要求下 金融机构加大移动端安全投入

“一直以来，金融行业都有自身需要面对的安全问题，如盗转、盗刷等，这些问题在移动互联时代更加明显。此外，金融行业是对安全级别要求最高的行业之一，从身份认证方式、国家密码算法使用、等级保护标准等各方面都有相应的要求。因此，近几年金融机构对业务安全的需求也逐渐增长。”12 月 12 日，北京芯盾时代科技有限公司副总裁蔡准在接受记者采访时表示。

“越来越多银行的业务从 PC 端转移到了移动端，尤其对中小银行来说，线下营业厅的成本相对较难负担，因此对手机端更加看重，许多业务都转移到线上来做了，在手机端购物和转账的操作也越来越多。”据蔡准介绍，芯盾时代主要的客户群就是金融机构客户，“我们 300 多个客户里有 200 多个客户是银行，还有不少是证券公司和保险公司。在移动应用的场景下，许多金融机构客户需要在手机端拥有足够安全的身份认证措施，这类认证措施在以前是 U 盾，但由于手机无法使用 U 盾，而人民银行和银监会对 5 万以上的转账额度又有相应

的监管文件要求，因此我们就提供了能够符合监管要求的多因素认证产品，让 App 的支付额度能够从几千元提高到二三十万。”

12 月 13 日，奇安信集团副总裁梁志勇对记者表示，信息化建设与合规需求是企业投入安全建设的两大原因。“现在很多企业都有做大数据、云计算的需求，而这些都附带有安全的要求。此外，国家也提出了很多需要企业达标的硬性标准。而不同行业的企业，也需要达到各自不同的垂直性很强的行业标准，银行、公安等系统都是如此。”

蔡准告诉记者，从 2016 年开始，银监会明确发文对普通转账要求进行短信验证，并要求对短信验证进行保护。2017 年则对银行的风控系统提出了要求，这导致了 2018 年和 2019 年成为了银行风控系统建设的高峰期。与此同时，等保 2.0 标准也对移动终端提出了更高的要求体系。可以看到各个机构都意识到了互联网业务面临的风险，需要金融机构采用对应的防控措施。

根据央行发布的“237 号文”，央行对移动金融 App 安全问题进行管理规范，主要从提升安全防护、加强个人金融信息保护、提高风险监测能力、健全投诉处理机制、强化行业自律 5 个方面入手，并对备受关注的个人金融信息保护划定了四大红线。

多位金融行业受访者对记者表示，受各类标准出台的影响，金融安全需求在近几年持续增多，金融行业不断在安全层面加大投入。

“我们在银行成立的第一天开始，科技部下面下设了一个独立的大数据中心，专职做数据的平台建设工作，数据治理的工作，目前我们行里面自己的开发人员大概 200 人左右，大数据开发人员占到 1/3，数据对我们来说是核心资产。此外，在信息安全上的投入，相对来说我个人认为也是比较大的，尽管现在我们全行的开发人员才 200 人，但是专职的信息安全人员已经 20 人了，风险部门还有一个专职的反欺诈的团队，他们更多是做业务安全，我们科技这边更多的是做信息安全，几个不同的层次强化数据安全的保护工作。”新网银行信息科技部负责人周勇在“2019 新京报金融科技论坛”上表示。

“前不久央行发文指导互联网金融协会启动了金融 App 的备案管理试点工作，简单来说，就是对金融类 App 开展标准测评和认证，实施动态监测，及时处置相关风险。”央行科技司司长李伟 12 月 11 日表示，加快标准供给的同时，也在积极推进标准的落地实施，把金融科技标准实施与加强金融科技创新监管相结合，通过标准、测评和认证三个环节的工作规范金融科技创新应用，提升金融科技的监管效能。

银行遭遇互联网黑产 提高风控水平成课题

蔡准告诉记者，安全公司为金融机构提供安全技术支持的具体方式是集成一个 SDK 到

银行的 App 中，“我们 SDK 索要的权限只要银行 App 本身要求开启的权限即可，没有额外要求。”

根据中国信息通信研究院发布的《2019 金融行业移动 App 安全观测报告》，截至 2019 年 9 月 11 日，该报告团队从 232 个安卓应用市场中收录了 13.33 万款金融行业 App，发现有 70.22%的金融行业 App 存在高危漏洞，攻击者可利用这些漏洞窃取用户数据、进行 App 仿冒、植入恶意程序、攻击服务等，对 App 安全具有严重威胁。其中 Top3 的高危漏洞均存在导致 App 数据泄露的风险。

“从银联卡支付到银联手机闪付，再到银联云闪付 App 以及二维码支付，随着时代的发展，目前风险也加速向线上移动端转移，向支付业务全链条全方位渗透，由单一风险向各类风险交织并存发展，金融科技与新型风险相结合，催生团伙犯罪以及黑色产业链条，增大了风控的压力。”12 月 14 日，中国银联法律合规部总经理郑晓琴在互联网安全与刑事法制高峰论坛上称。

那么，金融机构面对的风险主要有哪些？

在腾讯安全云鼎实验室负责人董志强看来，网点时代银行业的安全防护主要体现在业务连续性安全保障，集中在基础环境安全、网络连通性安全、应用安全等领域。而从网银时代开始，防止业务攻击和数据篡改、越权等安全防护成为了安全防护重点，同时针对普通用户银行账户的犯罪越来越多，如转账类诈骗、“四件套”交易等，这都需要银行方面有更强的监管能力。

微众银行反欺诈负责人诸劼称，薅羊毛对银行和互联网黑产来说都不是新鲜事，传统银行会遭遇套积分行为，互联网黑产则会经常薅电商的优惠券。但当金融机构逐步向移动端转移的过程中，银行碰到互联网黑产，就会出现问题。“银行没有见过这么大的账号群控黑产群体，而黑产则在电商外又找到一块大蛋糕。对于银行传统的注册账户必须手机验证和领券必须提供有效身份证的监管机制，互联网黑产往往可以使用大量手机号资源，接码平台以及大量身份信息去绕过，对此银行只能采取新方式对抗。”

蔡准对记者举例称，此前有一家银行上线了其提供的风控系统后，在其 App 的商城里拦截到一些商户的订单。“这些商户在该银行 App 里出售商品时，使用同一个设备购买自己的商品‘刷单’，以这样的方式来‘薅’银行为商户提供的交易补贴，该银行此前承受了两年的损失，采用了反欺诈系统后才发现问题。”

董志强表示，目前，随着移动网络时代开始，移动安全、云安全、数据安全成为防护重点，同时语音支付、人脸支付等方面，银行也会面临新的威胁，比如 AI 伪造语音、AI 伪造

人脸的攻击，如何对此类新型攻击做到有效防护，也是需要银行等机构进行持续性研究。

“从 2015 年至今，金融机构与黑产的‘战况’一直很胶着，这是因为移动互联领域涉及很多风险点，而且相关的技术一直在升级，道高一尺魔高一丈的事情一直在发生。银行除了自身的风控团队外，还需要安全技术人员的配合，未来希望有更多的法律法规出台可以保护金融机构的数据安全。”戴蒙表示。（来源：新华网）

➢ 数据安全：人工智能健康发展的核心命题

重习近平总书记“四个坚持”的重要指示，为“网络安全教育、技术、产业融合发展”和“人工智能、物联网、下一代通信网络等新技术新应用”指明了方向。“坚持促进发展和依法管理相统一”和“积极利用法律法规和标准规范引导新技术应用”的要求，是把握信息化发展大势、积极应对网络安全挑战的必然内涵。在网络强国建设的过程中，唯有将“四个坚持”落到实处，才能更加有力地维护人民群众在网络空间的切身利益，“提升广大人民群众在网络空间的获得感、幸福感、安全感”。

在云计算、大数据、机器学习、深度学习、人脑芯片等新一代信息技术的推动下，人工智能正以前所未有的速度、广度和深度融入社会生活的各个方面，成为全球新一轮科技革命与产业变革的发力点和着力点。人工智能时代，海量的数据将得到充分利用，因此，人工智能时代也被称为“数据驱动”时代，而利用海量数据实现巨大的商业和社会价值，已经引起广泛关注。我国于 2017 年颁布了《新一代人工智能发展规划》，将人工智能定义为国际竞争

的新焦点和经济发展的新引擎，将其正式提升至国家战略的高度，为新一代技术的研发、应用和推广提供了坚实的后盾。同时，该规划也明确提出，人工智能发展过程的不确定性将对法律秩序、伦理秩序、个人隐私等带来巨大的风险和挑战。

一、数据安全是人工智能安全的核心

在人工智能技术日新月异的时代，尽管人工智能在很多领域得到成功应用，但是，数据的安全管理滞后于技术的发展的现实，也引发人们的担忧。

人工智能的核心是数据，数据是人工智能时代生产资料和生产工具的集合，是经济社会发展的重要生产要素和国家基础战略性资产。一方面，海量的数据推动人工智能的发展；另一方面，人工智能也可以提高数据采集管理能力和数据挖掘利用水平。目前，政府和企业的决策越来越依赖大量的数据分析，包括政府经济、社会统计、企业商业营销等，大规模的数据收集、分析和使用，使传统社会走向透明化，同时，也伴随隐形的数据安全隐患。

数据安全是人工智能安全的关键与核心，数据的质量和安全直接影响人工智能算法和模型的准确性。人工智能的数据安全涉及技术、社会、法律等多个领域，一旦发生数据安全问题，其影响范围很难控制，不仅仅对公民个人，而且对企业、国家都可能造成难以估量的损失。海量数据又是人工智能时代数据的普遍特征，其在数据管理、应用等方面与传统数据安全显著不同，需要针对这些新情况、新问题研发针对性的数据安全防护技术，保证信息安全。

二、对人工智能数据安全的认识有待提升

各行各业对数据的重视程度很高，都在利用数据进行相关的分析和挖掘，从而做出最佳的决策。然而，对于人工智能的数据安全，当前普遍存在认识不足、保护不周的情况。

个人的数据安全保护意识有待提高。在网络平台随意注册账号，浏览不正规网站、下载未验证软件、有意无意传播个人信息，为获取个人利益而非法窃取、售卖他人信息等，网络用户的不规范行为屡见不鲜。

企业的数据安全保护有待加强。由于人工智能相关技术发展处于早期阶段且发展迅速，全球范围无论是大型科技企业，还是初创企业，投入大量资源开展人工智能技术的开发和应用研究，但是，企业对人工智能数据安全问题重视不够，除非出现数据泄露事件。

数据安全保护法律法规有待完善。面对人工智能数据的复杂性、多场景、多应用、信息交叉使用等特征，现有数据安全法律制度有待继续跟进更新。对人工智能时代网络环境的变化和数据泄露的多渠道性和多样性，现有的法律没有给予充分的认识。

数据安全缺乏有效的监管手段。人工智能技术存在算法黑箱，具有明显的不确定性，而数据安全的监管无法跟上人工智能技术的进步和发展，容易带来数据安全的隐患。人工智能

更加依赖数据，而数据在交叉引用过程中是否被污染，变得愈发难以鉴别。

三、人工智能数据安全面临的机遇和挑战

1．人工智能数据安全面临的机遇

促进数据安全治理的智能化和精准化。人工智能技术可以将数据安全研究人员从海量的威胁数据分析中解放出来，通过监测威胁可以迅速发现、分析和响应新攻击和新漏洞，实时共享威胁情报，实现系统自动防御修复，从而有效地推动数据安全治理更加自动化、智能化、高效化和精准化。

提高动态变化数据安全的监测防护。人工智能自动学习和自主决策能力可有效缓解现有数据安全技术手段对专业人员分析判断的高度依赖，实现对动态变化数据安全风险的自动和智能监测防护。

丰富数据安全的处理手段。人工智能卓越的海量数据处理能力，可有效弥补现有数据安全技术手段数据处理能力不足的缺陷，实现对大规模数据资产和数据活动的高效、精准管理和保护。

推动社会经济的数字化转型升级。人工智能技术赋能数据安全的监测防护，能够更大程度上助力数据大规模的安全应用，人工智能技术将有力推动经济社会的数字化转型升级。

2．人工智能数据安全面临的挑战

网络信息安全威胁加剧。无论是消费互联网还是社交互联网，个人信息将更多地保存和暴露在服务器上，虽然服务器会进行一定的数据安全防范，但是，这仍不可避免面临被攻击的风险。近年来，网络诈骗或电信诈骗案件持续高发，这类诈骗案件就是公民个人信息泄露带来的后果。

网络攻击形势更加严峻。人工智能大数据的特性使数据的价值密度有所下降，海量数据增加了数据安全防护的难度，数据安全人员若想从海量数据中寻找监测出具体的安全威胁，将变得难上加难，而当前的数据安全技术已经不能满足其需求，这使网络攻击更加容易。

法律法规与监管问题突出。人工智能技术的应用给传统行为带来强烈的冲击和挑战，例如，以往在金融服务领域应用的人脸识别技术，虽然其安全性比传统的认证方式有所提高，但是，仍不能保证准确率达到 100%，当出现错误时如何处理，造成的损失由谁承担等，往往很难界定。此外，人工智能的新应用、新商业模式层出不穷，相关法律法规的跟进、修订与制订等问题，显得更加突出。

四、建立健全人工智能数据安全规范体系

引导形成人工智能伦理规范。一方面，针对我国人工智能相关机构、行业和企业发布的

人工智能伦理规则规范，加强宣传力度，扩大影响范围，提升人工智能用户尤其是青少年的数据保护意识。另一方面，通过国际组织和平台，积极开展国际合作与对话，推动形成广泛共识的国际人工智能数据安全伦理规范。

健全人工智能数据安全法律法规。一方面，明确人工智能数据安全的法律原则，建立人工智能数据安全的问责制和救济制，推进人工智能相关法律的出台。另一方面，参照国家现有法律体系，根据人工智能在不同场景中的应用特点，制定和细化相关规章制度，提出对人工智能应用过程中数据安全的要求。

完善人工智能数据安全监管手段。一方面，依照国家法律法规，通过线上线下多种方式对人工智能数据安全风险进行监督检查，以便及时发现和防范安全隐患。另一方面，依托行业协会组织或第三方机构，建立人工智能数据安全检测评估平台，提升人工智能产品的安全性，降低人工智能数据安全风险

健全人工智能数据安全标准体系。一方面，在我国人工智能安全标准框架下，加快研制数据安全标准体系，制定人工智能数据安全标准推进计划，推进人工智能数据安全评估和保护工作。另一方面，成立以国家信息安全标准化技术委员会牵头的人工智能安全研究组，有序推进人工智能数据安全标准的出台。

创新人工智能数据安全技术方法。一方面，完善人工智能开源学习框架，构建保障数据安全的人工智能基础研发平台，加快培育自有人工智能开源平台共享应用产业链和生态圈。另一方面，鼓励相关企业发挥自有优势，成立联合实验室，开展人工智能技术在数据安全领域的应用研究和产品技术研发。

培养人工智能数据安全高端人才。一方面，鼓励高校形成人工智能与信息安全交叉学科的人才培养模式，壮大师资队伍，同时，鼓励企业内部创办培训机构，或采用校企联合的方式，加强培训培育。另一方面，出台人工智能数据安全高端人才引进政策，支持高校和企业引进世界一流人工智能数据安全领军人才。（来源:《中国信息安全》杂志 2019 年第 11 期）

四、政府之声

➢ 中央网信办：全面提升网络安全防护能力 加强关键信息基础设施保护

2019 年 12 月 13 日，中央网信办召开主任办公会，传达学习中央经济工作会议精神，对抓好会议精神的贯彻落实作出部署安排。

会议要求，要紧密结合网信工作实际，立足于更好发挥网络舆论的“凝心聚力”作用、信息化的“赋能增效”作用、网络安全的“保驾护航”作用，为党和国家中心工作提供有力服务、支撑和保障，切实将总书记重要讲话精神落到实处。要用好网络传播“主阵地”，加强正面宣传和舆论引导，稳定预期、增强信心，唱响中国经济光明论，为经济发展营造良好网络舆论环境。要厚植数字经济发展“动力源”，深入实施《数字经济发展战略纲要》，着力解决核心技术“卡脖子”问题，加强信息基础设施建设，深入开展网络扶贫行动，促进互联网企业更加健康有序发展，为经济发展提供有力信息化支撑。要筑牢网络安全“防火墙”，全面提升网络安全防护能力，加强关键信息基础设施保护，加快制定出台相关法律法规，依法严厉打击网络违法犯罪行为，为经济发展提供可靠网络安全保障。

中央纪委国家监委驻中宣部纪检监察组有关负责同志及办各局、机关党委，有关直属单位主要负责同志参会。（来源：网信中国）

➢ 工信部《工业互联网企业网络安全分类分级指南（试行）》公开征求意见

2019 年 12 月 17 日，为贯彻落实《加强工业互联网安全工作的指导意见》，推动工业互联网安全责任落实，对工业互联网企业网络安全实施分类分级管理，提升工业互联网安全保障能力和水平，工信部研究起草了《工业互联网企业网络安全分类分级指南（试行）》（征求意见稿）。现向社会公开征求意见。

工信部表示：有三类企业适用于本指南：1. 应用工业互联网的工业企业；2. 工业互联网平台企业（主要指对外提供工业互联网平台等互联网信息服务的企业）；3. 工业互联网基础设施运营企业，主要包括基础电信运营企业和标识解析系统建设运营机构。

此外，工信部表示，本次指南的基本原则包括：企业分级与行业网络安全影响程度相关联、行业指导与地方监管相结合、企业自评与属地核查相结合等。（来源：工信部网站）

- **工业互联网企业网络安全分类分级指南（试行）（征求意见稿）全文：**
- http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057728/c7571643/content.html

➢ 七部门联合下发《关于促进“互联网+社会服务”发展的意见》

2019 年 12 月 12 日，国家发展改革委、教育部、民政部、商务部、文化和旅游部、卫生健康委、体育总局七部门联合下发《关于促进“互联网+社会服务”发展的意见》（简称《意见》发改高技〔2019〕1903 号。《意见》提出，推进社会服务资源数字化，激发“互联网+”对优质服务生产要素的倍增效应。鼓励发展互联网医院、数字图书馆、数字文化馆、虚拟博物馆、虚拟体育场馆、慕课等，推动社会服务领域优质资源放大利用、共享复用。加大社会服务领域数据共享开放力度，提升数据资源利用效率。优先推进文化、旅游、体育、医疗等领域公共数据开放。并推进社会服务主体数字化转型，有效提升资源匹配效率。（来源：国家发展改革委高技术司）

- **《关于促进“互联网+社会服务”发展的意见》发改高技〔2019〕1903 号**
- **全文：**https://www.ndrc.gov.cn/xxgk/zcfb/tz/201912/t20191212_1213336.html

➢ 国家网信办发布《网络信息内容生态治理规定》

2019 年 12 月 20 日，国家互联网信息办公室发布了《网络信息内容生态治理规定》(以下简称《规定》)，自 2020 年 3 月 1 日起施行。国家互联网信息办公室有关负责人表示，出台《规定》，旨在营造良好网络生态，保障公民、法人和其他组织的合法权益，维护国家安全和公共利益。

党的十九届四中全会《决定》中明确提出，建立健全网络综合治理体系，加强和创新互联网内容建设，落实互联网企业信息管理主体责任，全面提高网络治理能力，营造清朗的网络空间。加强网络生态治理，是建立健全网络综合治理体系，培育积极健康、向上向善的网络文化的需要，也是维护广大网民切身利益的需要。

《规定》提出，鼓励网络信息内容生产者制作、复制、发布含有“宣传习近平新时代中国特色社会主义思想，全面准确生动解读中国特色社会主义道路、理论、制度、文化”和“弘

扬社会主义核心价值观，宣传优秀道德文化和时代精神，充分展现中华民族昂扬向上精神风貌”等内容的正能量信息。网络信息内容生产者不得制作、复制、发布含有“危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一”和“损害国家荣誉和利益”等内容的违法信息，应当采取措施，防范和抵制制作、复制、发布含有“使用夸张标题，内容与标题严重不符”和“炒作绯闻、丑闻、劣迹”等内容的不良信息。

《规定》强调，网络信息内容服务平台应当履行信息内容管理主体责任，加强本平台网络信息内容生态治理，培育积极健康、向上向善的网络文化。网络信息内容服务平台应当建立网络信息内容生态治理机制，制定本平台网络信息内容生态治理细则，健全用户注册、账号管理、信息发布审核、跟帖评论审核、版面页面生态管理、实时巡查、应急处置和网络谣言、黑色产业链信息处置等制度。

《规定》要求，网络信息内容服务平台不得传播本规定第六条规定的违法信息，应当防范和抵制传播本规定第七条规定的不良信息。网络信息内容服务平台应当加强信息内容的管理，发现本规定第六条、第七条规定的信息的，应当依法立即采取处置措施，保存有关记录，并向有关主管部门报告。鼓励网络信息内容服务平台坚持主流价值导向，优化信息推荐机制，加强版面页面生态管理，在重点环节积极呈现本规定第五条规定的正能量信息，不得在重点环节呈现本规定第七条规定的不良信息。

《规定》明确，网络信息内容服务使用者应当文明健康使用网络，按照法律法规的要求和用户协议约定，切实履行相应义务，在以发帖、回复、留言、弹幕等形式参与网络活动时，文明互动，理性表达，不得发布本规定第六条规定的违法信息，防范和抵制本规定第七条规定的不良信息。网络信息内容服务使用者和生产者、平台不得开展网络暴力、人肉搜索、深度伪造、流量造假、操纵账号等违法活动。

国家互联网信息办公室有关负责人指出，网络信息内容生态治理需要政府、企业、社会、网民等多方主体参与，共同构建良好的网络生态，营造清朗的网络空间。（来源：国家互联网信息办公室）

- **《网络信息内容生态治理规定》**
- **全文：**http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm

五、本期重要漏洞实例

➢ Adobe Acrobat 及 Reader 任意代码执行漏洞

发布日期：2019-12-10
更新日期：2019-12-12
受影响系统：
Adobe Acrobat Reader DC <= 2019.021.20056
Adobe Acrobat DC <= 2019.021.20056
Adobe Acrobat 2017 <= 2017.011.30155
Adobe Acrobat 2017 <= 2017.011.30152
Adobe Acrobat Reader 2017 <= 2017.011.30152
Adobe Acrobat 2015 <= 2015.006.30505
Adobe Acrobat Reader 2015 <= 2015.006.30505
描述：

CVE(CAN) ID: CVE-2019-16453
Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Reader 是一套 PDF 文档阅读软件。
Adobe Acrobat 和 Reader 在实现中存在安全限制绕过漏洞。攻击者可利用该漏洞执行任意代码。
<*来源：HTBLA Leonding
链接：https://helpx.adobe.com/security/products/acrobat/apsb19-55.html
*>

建议：

厂商补丁：
Adobe

Adobe 已经为此发布了一个安全公告（APSB19-55）以及相应补丁：
APSB19-55：Security update available for Adobe Acrobat and Reader
链接：https://helpx.adobe.com/security/products/acrobat/apsb19-55.html

➢ IBM SmartCloud Analytics 信息泄露漏洞

发布日期：2019-12-07
更新日期：2019-12-10
受影响系统：
IBM SmartCloud Analytics 1.3.1 - 1.3.5
描述：

CVE(CAN) ID: CVE-2019-4214
IBM SmartCloud Analytics 是快速分析应用数据的日志分析解决方案。
IBM SmartCloud Analytics 1.3.1 - 1.3.5 版本，在授权标志或会话 cookie 的安全属性设置中存在不正确授权漏洞。通过中间人攻击，攻击者可利用该漏洞获取敏感信息。

<*来源：vendor
*>

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/1110171
https://exchange.xforce.ibmcloud.com/vulnerabilities/159185

➢ GE S2020/S2020G Fast Switch 61850 跨站脚本漏洞

发布日期：2019-12-17
更新日期：2019-12-19
受影响系统：
General Electric S2020/S2020G Fast Switch 61850 <= 07A03
描述：

CVE(CAN) ID: CVE-2019-18267
GE S2020/S2020G Fast Switch 61850 是管理型以太网交换机。
S2020/S2020G Fast Switch 61850 07A03 及之前版本，在实现中存在跨站脚本漏洞，攻击者可以将任意 Javascript 注入特制的 HTTP 请求中，并可能会反映在 HTTP 响应中。该设备还容易受到存储型跨站脚本漏洞的攻击，该漏洞可能允许会话劫持，敏感数据泄露，跨站点请求伪造攻击和远程执行代码。

<*来源：Murat Aydemir

链接：https://www.us-cert.gov/ics/advisories/icsa-19-351-01
*>

建议：

厂商补丁：
General Electric

目前厂商已经发布了版本 07A04，修复了这个安全问题，请到厂商的主页下载：
https://www.gegridsolutions.com/app/ViewFiles.aspx?prod=S20&type=7

➢ Microsoft Access 信息泄漏漏洞

发布日期：2019-12-10
更新日期：2019-12-12
受影响系统：
Microsoft Office 365 ProPlus
Microsoft Office 2019
Microsoft Office 2013 SP1
Microsoft Office 2013 RT SP1
Microsoft Office 2010 (64-bit edition) SP2
Microsoft Office 2010 (32-bit edition) SP2
描述：

CVE(CAN) ID: CVE-2019-1400

Microsoft Office Access 是由微软发布的关系数据库管理系统。
Microsoft Access 软件无法正确处理内存中对象时，该软件中存在信息泄漏漏洞。成功利用此漏洞的攻击者可以获取信息，从而进一步入侵用户系统。

<*来源：Microsoft
*>

建议：

厂商补丁：
Microsoft

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://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-1400

六、本期网络安全事件

➢ Elasticsearch27 亿数据泄露 10 亿明文波及中国大厂

2019 年 12 月 12 日，又是让人无语的 Elasticsearch 服务器，不到两周时间，新一轮的数据泄露事件便再度发生，这次，研究人员在不安全的云存储桶中，总共发现了 27 亿个电子邮件地址，10 亿个电子邮件账户密码以及一个装载了近 80 万份出生证明副本的应用程序。研究人员称，过去一年里，一些企业无意识得让他们的 Amazon Web 服务 S3 和基于云计算的 ElasticSearch 存储桶暴露出来。它们没有任何适当的安全措施，也没有被试图锁定的迹象。

SecurityDiscovery 网站的网络威胁情报总监鲍勃·迪亚琴科（Bob Diachenko）称，我们在上周发现了一个巨大的 ElasticSearch 数据库，包含超过 27 亿个电邮地址，其中有 10 个的密码都是简单的明文。大多数被盗的邮件域名都来自中国的邮件提供商，比如腾讯、新浪、搜狐和网易。当然，雅虎 gmail 和一些俄罗斯邮件域名也受了影响。这些被盗的电邮及密码也与 2017 年那次大型的被盗事件有关，当时有黑客直接将它们放在暗网上售卖。

该 ElasticSearch 服务器属于美国的一个托管服务中心，后者在 Diachenko 发布数据库存储安全报告后于 12 月 9 日被关闭。但即使如此，它已经开放了至少一周，并且允许任何人在无密码的情况下进行访问。

Diachenko 称，单就数字而言，这可能是我所看到的记录数据最庞大的一次（他自 2018 年以来发掘了多次数据泄露事件，其中包括 2.75 亿个印度公民信息的数据库）。

被泄露的 27 亿个电子邮件地址目前无法证实是否为有效地址，但其来源确属违规。Diachenko 认为，这些电子邮件往往不会引起企业的重视，但实际上电子邮件账户会受到攻击的可能性更高。因为这些电子邮件一旦引发攻击行为，用户通常不会受到警报，原因在于国内的防火墙阻止了检查电子邮件泄露的服务。

目前尚不清楚到底谁公开了数据库，这有可能是黑客，也有可能就是安全研究人员。但无论哪种方式，该行为都忽视了 ElasticSearch 原本提供的安全性选项，这只是许多忽略保护云存储安全重要性示例中的另一个。

Diachenko 在研究中发现一个线索，数据库的所有者用每个地址的 MD5、SHA1 和 SHA256 散列对偷来的电子邮件地址进行了操作，这很有可能是为了方便在数据库中进行搜索。这种情况很像是原本买下了该数据库的某人本试图启动其搜索功能，却被错误配置成了公开可用。

与此同时，英国渗透测试公司 Fidus Information Security 的研究人员在 AWS S3 存储桶中发现了近 80 万份美国出生证明复印件的在线申请，该存储桶属于一家提供出生和死亡证明复印件服务的公司。bucket 没有密码保护，因此对任何人都是开放的。

有趣的是，据 TechCrunch 称，研究人员无法访问存储桶中的 94000 个死亡证明副本应用程序数据库。TechCrunch 发现，该应用程序中包含的数据可以追溯到 2017 年末，泄露数据的范围包括姓名、出生日期、地址、电子邮件地址、电话号码和其他个人数据。

Fidus 主管 Andrew Mabbitt 称，他的公司在从事 AWS S3 项目时发现了数据。该存储桶经过配置，可以实现对外界的开放可读，允许具有 URL 的任何人获得所有文件的完整列表。

截止目前，该程序库仍然保持公开状态。研究人员称，在多次联系 Amazon AWS 安全团队后，后者表示已将报告传递给存储桶所有者，并建议尽快采取措施。但是，所有者似乎忽略了这些消息，至今没有任何回复。位于公共互联网上的配置错误和暴露的数据，足以造成攻击事件发生。黑客可以对所有者进行信息欺诈或者盗取身份信息，这类有针对性的电子邮件网络钓鱼和黑进账户的案例已经很多。

Bitglass 的首席技术官 Anurag Kahol 建议，企业应确保他们对客户数据有充分的了解和把控度。适当得采用实时访问控制、静态数据加密并配置可以检测任何配置错误的云安全设置。（来源：雷锋网）

➢ 黑客攻破美一女孩房间安全摄像头并称自己是圣诞老人

2019 年 12 月 14 日，据外媒报道，有人黑进了美国密西西比一户人家的环形安全摄像头，并且还用扬声器骚扰这家的 8 岁女孩。这名黑客告诉她自己是圣诞老人并还怂恿她破坏房间。这是近期发生的几起黑客在用户不知情的情况下登陆其 Ring 账号的攻击事件之一。

Ashley LeMay 近日告诉媒体，她在自己女儿房间里安装了摄像头，这样她就可以在上夜班时照看她们。“在我买到它们之前做了很多研究。你知道，我真的觉得它是安全的。”

然而这次入侵就发生在她安装这款摄像头四天后，当时她正在出差，她的丈夫在家带孩子。当她的女儿 Alyssa 听到自己卧室传出来声音后于是走进去看看究竟是什么。

从当事人分享的视频可以看到，Alyssa 非常紧张地站在自己的房间里，黑客则远程播放了来自恐怖片《潜伏》里的歌曲《Tiptoe through the Tulips》。

“谁在那里，”Alyssa 问道。

“我是你最好的朋友。我是圣诞老人。我是圣诞老人。难道你不想成为我最好的朋友吗？”黑客说道。

之后，这个匿名黑客继续骚扰 Alyssa、嘲笑她并怂恿她破坏房间。对此，这款摄像头厂商 Ring 在提供给媒体的声明中指出，黑客并不是通过数据泄露或破坏 Ring 的安全获取信息的，相反，这个人可能利用了这户人家账户的安全性。

根据声明，Ring 用户经常会使用相同的用户名和密码来注册不同账户和订阅服务。“作为预防措施，我们强烈并公开鼓励所有 Ring 用户在其 Ring 账户上启用双重认证、添加共享用户（而不是共享登录凭证）、使用高安全性密码并定期更换密码。”Ashley 表示，她还没有

在她的设备上设置双重认证。（来源：cnBeta）

➢ 南通 6000 人抢“神盘”遭遇系统崩溃 开发商称黑客入侵引质疑

2019 年 12 月 11 日，中兴兰溪荟是一个位于南通开发区的楼盘，由于开盘价大幅低于周边二手房均价，今年 12 月 7 日 570 余套新房开盘时，吸引了 6000 余名市民前来摇号选房。但在摇号过程中，许多购房者发现，摇号系统严重卡顿，继而崩溃白屏，无法选房。对此，开发企业给出的答复是“遭到黑客侵入”，引发质疑。对此，南通市开发区房管部门称，已成立调查组对此事进行调查。

市民：锁资 80 万元抢购“神盘” 却遭遇“系统卡顿”无法选房

中兴兰溪荟小区位于南通开发区，今年 12 月 3 日取得了楼盘 97 至 100 栋，共 576 套住宅的预售许可证。12 月 4 日傍晚，开发商南通兴通智慧产业园建设有限公司突然通过微信通知购房者，必须前往开发区某银行办理银行卡并存入 80 万元意向金后，才能取得购房摇号资格。12 月 6 日凌晨，大量市民自带棉被，彻夜在银行门口排队，等待天亮办理锁资手续。

12 月 6 日上午，验资银行门前已经人山人海

但是，在 12 月 7 日选房过程中，许多市民表示，早在选号前，选房系统就已经出现了无法刷新、以及卡顿、崩溃的情况，因此怀疑选号结果有内定嫌疑。12 月 9 日下午，我记者就此致电南通市经济开发区房产管理局房管科进行咨询，工作人员表示，局领导正在就此事召开会议讨论解决办法。“这个事情蛮奇怪的，一共六千多个人摇号，好像只有四到五个人拿到房号。”这位工作人员介绍，“我这边是办公室，他们都去开会了，就是为兰溪荟的事情。”

但是，根据网络流传的一份选号成功者的名单，记者拨打了十余位已经成功取得购房资格的市民的电话，向他们咨询当天选号时是否存在微信选房系统卡顿崩溃的情况，但他们都表示，当天选房一切正常，非常顺利。“我……我点的快。”一位购房者表示。而另一位购房者则说：“后来的确存在这样的情况，但是当时我们已经选出房子了。所以没受影响。”

开发商：选房时有黑客攻击 当地已成立调查组介入调查

由于该楼盘开盘价大幅低于周边二手房均价，摇号结果的真实性引起了众多市民的关注。就在当天选房的公平性遭到许多购房者质疑后不久，开发公司南通兴通智慧产业园建设有限公司发布了一份申明，申明称，当天的销售过程中“发现有黑客侵入现象，导致系统缓慢”。

既然有黑客入侵摇号系统，此次摇号结果是否应该取消？当天又是否有公证处工作人员在摇号现场监督？我记者分别致电兰溪荟楼盘售楼处、开发公司南通兴通智慧产业园建设有限公司和此次购房摇号监督负责人程经理的电话，均无人接听。

申　明

我司郑重申明，我司房屋销售信息一律以我司公众号为准。我司除收取房款以外，其它不收取任何费用。我司从未委托任何中介公司进行房屋售卖业务。如有中介或第三方以我司名义收取任何茶水费、中介费等额外费用，我司将追究其法律责任。

我司在销售过程中发现有黑客侵入现象，导致系统缓慢。现特告知购房者，一旦发现黑客入侵，我司将取消相关购房者的购房资格，同时我司将依法报案，追究法律责任。

南通兴通智慧产业园建设有限公司

2019 年 12 月 9 日

12 月 10 日，记者再次联系南通开发区房管局，对方表示，开发区已成立多部门联合调

查组，对此次购房摇号中可能存在的问题进行调查。“现在已经成立了一个调查组，是管委会层面成立的，多部门联合参与。”而面对记者网上传言是否属实的疑问，这位工作人员表示还不清楚。“现在就要对这种情况进行核实，看看哪些说法是属实的，哪些是谣言。”

律师观点：真遭黑客攻击应重新选号

“遭到黑客攻击系统崩溃，最后产生的损失其实是消费者的交易机会。” 南京天煦律师事务所律师张赛认为，目前来看，6000 余名选房的购房者都预存了 80 万意向金，却没有得到一个公平的交易环境和均等的交易机会。如果有黑客侵入选房系统，开发商应该公示有力的证据后，重新进行摇号，而不是依然维持现在的选房结果，否则就是违反了诚实信用原则。“我个人认为，应当是重新选号。”（来源：江苏广电总台）

➢ 英国央行内部系统曾遭入侵 会议音频被窃取并卖给高频交易员

2019 年 12 月 19 日，据英国《泰晤士报》报道，英国央行的内部系统遭到劫持，导致有对冲基金获取英国央行还未在新闻发布会上公布的内容，并将这些机密信息用于高频交易，从中获取高达上百万美元的暴利。此外，该银行近期也发现，有机构未经同意就将英国央行新闻发布会的音频摘要提前发送给交易员。来看一下，到底发生了什么？

英国央行被“黑”

据《泰晤士报》报道，对冲基金一直在窃听英格兰银行(Bank of England)的信息，他们劫持了内部系统，这些信息只有在新闻发布会上才会正式发布。据《泰晤士报》的调查，英国央行发现，其一家设备供应商向高速交易员发送了其新闻发布会的音频源，这些交易员希望通过比其他人更早、更快地获取央行官员的言论，并以此从资本市场获利。

能够提前听到英国央行行长马克卡尼(MarkCarney)和其他高级官员的谈话，那怕仅仅只有几秒钟，对于快速交易员来说，就能获取丰厚的利润。卡尼在世行新闻发布会上的言论，经常能够推动英镑和黄金市场的波动。

英国央行表示，他们已经发现，自今年年初以来，一家第三方供应商滥用某些新闻发布会的音频源，向其他外部客户提供服务。据了解，第三方供应商与市场新闻服务相连，该服务承诺客户将比竞争对手更早地获得信息，而那怕只是早几微秒，该领域的信息也可以让信息优势者获取巨大利润。

该行的官方新闻发布会视频源由彭博社管理。然而，几年前，该行雇用承包商安装单独的备份音频源，以防视频源停机。除非视频失败，否则它从未打算被局外人使用。

资料显示，至少从今年年初开始，一家供应商侵入了音频源，并为其他公司提供该服务。文件显示，这项服务随后被出售给高速交易公司。

该行表示，已经暂停第三方供应商进入许可。一名发言人补充说，在银行不知情或者未经银行同意的情况之下，这种行为是完全不能接受的。相关情况还在进一步调查当中。

发言人表示：“英国央行在发布其政策委员会对市场敏感的决定时，以最高的信息安全标准运作。上述问题只涉及在此类声明之后举行的新闻发布会的广播。”

美联储也被窃听？

英格兰银行(Bank of England)的系统被滥用，使一组交易员比另一组交易者更有优势，这一消息将令其尴尬。因为央行的作用之一是支持公平和高效的市场。但受害者并不只有英国央行一家。据说，欧洲央行、美联储和加拿大央行的新闻发布会也有高速音频服务提供。

音频比视频更容易压缩和传输，让购买音频的交易者在市场上，获得了比其他交易者早 5 到 8 秒的时间。市场新闻服务除了收取订阅费外，每个客户每次新闻发布会的费用在 2500 英镑到 5000 英镑之间。但这么短的时间和这么少的费用却可以产生数以百万美元计的丰厚收益。这也是高频交易的生存之道。

金融危机后，随着对冲基金和投资银行寻找低风险回报，高频交易开始蓬勃发展。市场的分化在创造机会，Jump Trading， Optiver， Getco and Flow Traders 等公司一直都在英国各

地安装微波发射机。

高频交易是一项著名的对冲基金策略。除了上述公司外，很多对冲基金公司在英国各地的塔楼上安装了微波发射机，以在官方价格变动前几秒钟获取市场信息。这种手段在体育博彩中也十分常见。通过发送“观察者”到世界各地正在举办的赛事活动，如网球比赛，这样他们就可以在线上博彩应用程序之前发布信息，从而能够提高他们的胜率。

金融体系安全值得警惕

从目前的情况来看，英国金融体系的确存在一些漏洞。今年 8 月，伦敦富时 100 指数(FTse100)在欧洲股市开盘时未能开盘。直到 100 分钟之后，伦敦证交所才宣布开盘。根据一份官方声明，伦敦证交所(LSE)正在调查一个潜在的交易服务问题。而这已经不是第一次出现这样大的故障，2018 年 6 月，该交易所曾因软件问题而推迟开盘一小时。而在此之前，还出现过类似的情况。

而从全球范围来看，金融机构也一直是黑客觊觎的地方。2015 年 2 月 15 日，俄罗斯杀毒软件供应商卡巴斯基实验室(Kaspersky Lab)在日前发布的报告中指出，一家神秘的黑客组织对全球超过 100 家银行和金融机构进行了秘密攻击，并盗窃了 3 亿美元资金。

美国时间 2016 年 9 月 1 号凌晨 3 点，发生了一起银行网络盗窃案件，损失达 20 亿美元，一名黑客发现美国某银行中心服务器存在漏洞，很容易就攻击进入了银行系统内部，原因既然是服务器防火墙设置有问题。

据报道，欧洲央行今年 8 月关闭了一个由第三方供应商托管的外部网站，黑客攻击了保护其银行综合报告辞典(BIRD)网站的安全措施，导致部分用户的电子邮件地址和其他联系数据泄露。但欧洲央行强调，其内部系统和对市场敏感的信息并未泄露。

据凤凰网，除了欧洲外，亚洲国家的央行也曾遭黑客入侵，而遭到攻击的正是全世界绝大多数银行都在使用的 SWIFT 结算系统。据报道，2018 年 2 月，孟加拉央行被黑客盗走 8100 万美元，引起了全球储户的高度关注和恐慌。（来源：券商中国）

➢ 加拿大实验室 LifeLabs 付钱给黑客以恢复 1500 万客户的数据

2019 年 12 月 19 日，引述外媒报道，加拿大领先的实验室诊断和测试服务提供商 LifeLabs 今天承认，已向黑客支付报酬，以检索在上个月发生安全漏洞期间被盗的数据。

该公司今天在新闻稿中说：“我们与熟悉网络攻击并与网络犯罪分子进行谈判的专家合

作，向黑客支付了费用。”

目前尚不清楚该公司为恢复其数据支付了多少费用。通过电话与 LifeLabs 发言人联系时，不会立即对其发表评论。

根据与提交的文件信息办公室和安大略省的私隐专员及信息办公室和私隐专员不列颠哥伦比亚省，安全漏洞上个月发生的，围绕 11 月 1 日。

LifeLabs 说，黑客破坏了其系统，提取了客户数据，然后要求赎金将公司的数据还给公司。据 LifeLabs 称，黑客窃取了超过 1500 万客户的信息。攻击者窃取的个人数据类型包括姓名，家庭地址，电子邮件地址，用户名，密码和健康卡号。对于 85,000 个客户，还包括医疗测试结果。LifeLabs 说，被盗的数据是 2016 年或更早的日期。

这家加拿大公司表示，目前正在与执法部门合作调查这次黑客行为。它还说，它为曾经破坏其服务器的入口点黑客修补了其系统。

“我想强调的是，目前，我们的网络安全公司已建议与此次网络攻击相关的客户风险较低，并且他们没有将任何公开的客户数据披露为调查的一部分，包括监视暗网和其他在线位置。” LifeLabs 总裁兼首席执行官 Charles Brown 说。（来源：cnBeta）

➢ 北美数十家加油站 POS 刷卡系统被黑客组织攻破

2019 年 12 月 21 日，，近期北美已经有数十家加油站收到了 Visa 公司的警告通知，称他们的 POS 刷卡系统已经被臭名昭著的黑客组织 FIN8 攻破，使得持卡人在加油站刷卡之后，Visa 卡的银行账号被黑客侵入。

最早，Visa 公司发现 POS 刷卡系统被侵入是在今年的 8、9 月份。紧接着在 11 月份，

Visa 卡在加油站被黑的案件连续爆发了十几起，使得 Visa 公司不得不紧急对外发布公开警告。

根据 Visa 的官方通告，这次加油站侵入盗卡比之前的读卡器盗卡手法要更先进。之前的“Skimming”读卡器盗卡技术，是犯罪分子在刷卡机的读卡器里安装一个读卡器设备，顾客一旦插卡消费后银行卡信息就会被读卡器读走，进而导致银行账户信息发生泄漏。

而这次的加油站盗刷，黑客们完全不需要安装任何读卡设备，而是直接黑进了加油站的 POS 刷卡机系统，只要顾客在刷卡机上刷卡操作成功，银行卡信息就被远在千里之外的黑客盗走了。

这次黑北美加油站刷卡机的黑客组织 FIN8，这是一个喜欢针对零售、酒店和医院的黑客组织。那么他们到底是怎么黑进加油站的 POS 刷卡系统的呢？Visa 卡的官方通告里称，主要是加油站里与 POS 刷卡系统相连的电脑被黑客利用钓鱼邮件或软件给侵入了。大多数这些手法都极其隐蔽，被黑之后加油站电脑看起来仍然很正常，但是只要有油泵付款机上 Visa 卡的刷卡动作，银行卡信息就会立即被黑客窃取。

Visa 公司声称，黑客能够完成入侵也跟部分加油站刷卡系统升级更新较慢有关。当前最安全的刷卡方式是芯片读取模式，但是北美有部分加油站还是在继续使用老式的划卡系统。而划卡系统相比于芯片读取系统来说，安全系数较低，也更容易被黑客攻破。

因此，为了防止加油站 Visa 卡被黑事件再度升级，Visa 公司已经通知了所有加油站合伙伙伴，希望他们在 2020 年 10 月以前全部更换掉划卡 POS 系统，将其升级为芯片读卡刷卡系统。Visa 公司将会负责赔付在这个时间点之前的所有加油站 Visa 卡被盗刷的损失，但

明年 10 月份过后该公司就将不再赔付，需要加油站来承担顾客银行卡被盗刷的损失。

说完了加油站黑客，老白再给大家分享一个加油省钱小妙招！到底大家该在一周当中的什么时候加油最超值呢？快来一起看看吧。

根据 GasBuddy 网站公布的最新统计数据，发现在加拿大的大部分地区，工作日的第二天即每周二，通常是加油最超值的时间（尤其是晚上 9 点以后）,而周五的平均油价一般是一周中最贵的。所以小伙伴们可以在每周二检查一下油表，需要的话可以在晚上回家的路上顺便也给爱车填饱肚子吧。（来源：科技生活快报）