国盟信息安全通报

2020 年 9 月 13 日第 224 期

全国售后服务中心

国盟信息安全通报

（第 224 期）

国际信息安全学习联盟

2020 年 09 月 13 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 465 个，其中高危漏洞 131 个、中危漏洞 274 个、低危漏洞 60 个。漏洞平均分值为 5.73。本周收录的漏洞中，涉及 0day 漏洞 77 个（占 17%），其中互联网上出现“WordPress Vanguard 跨站脚本漏洞、Metasploit Framework 相对路径遍历漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3165 个，与上周（4604 个）环比减少 45%。

主要内容

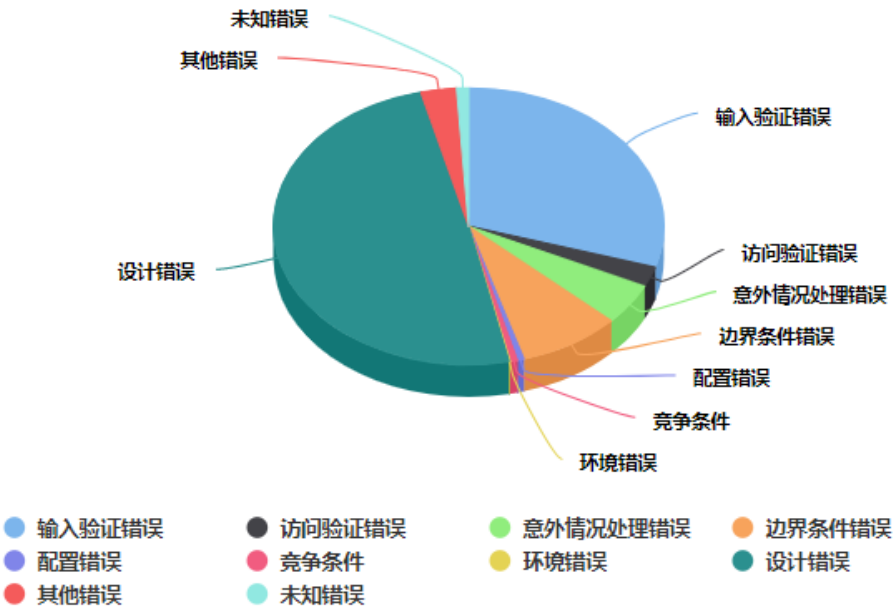
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

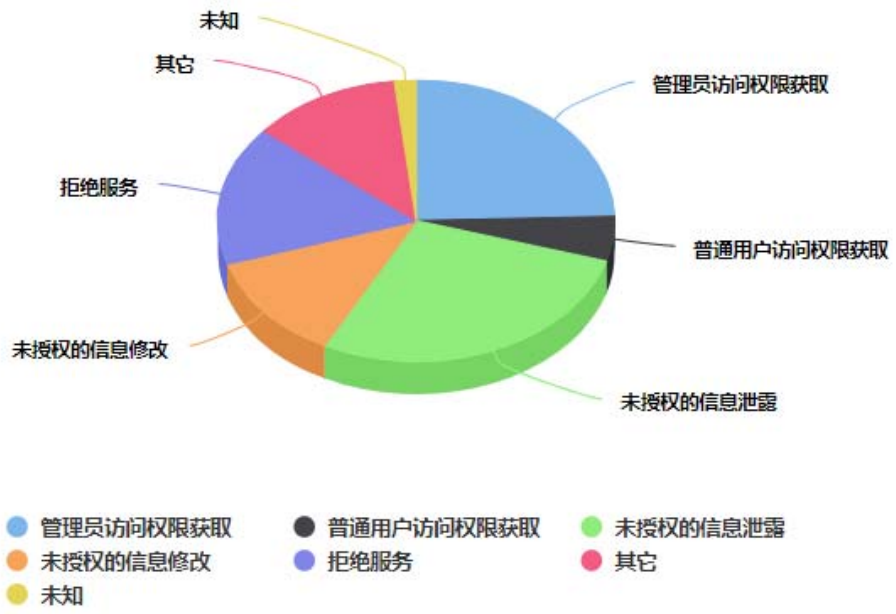
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 465 个，其中高危漏洞 131 个、中危漏洞 274 个、低危漏洞 60 个。漏洞平均分值为 5.73。本周收录的漏洞中，涉及 0day 漏洞 77 个（占 17%），其中互联网上出现“WordPress Vanguard 跨站脚本漏洞、Metasploit Framework 相对路径遍历漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3165 个，与上周（4604 个）环比减少 45%。

二、安全漏洞增长数量及种类分布情况

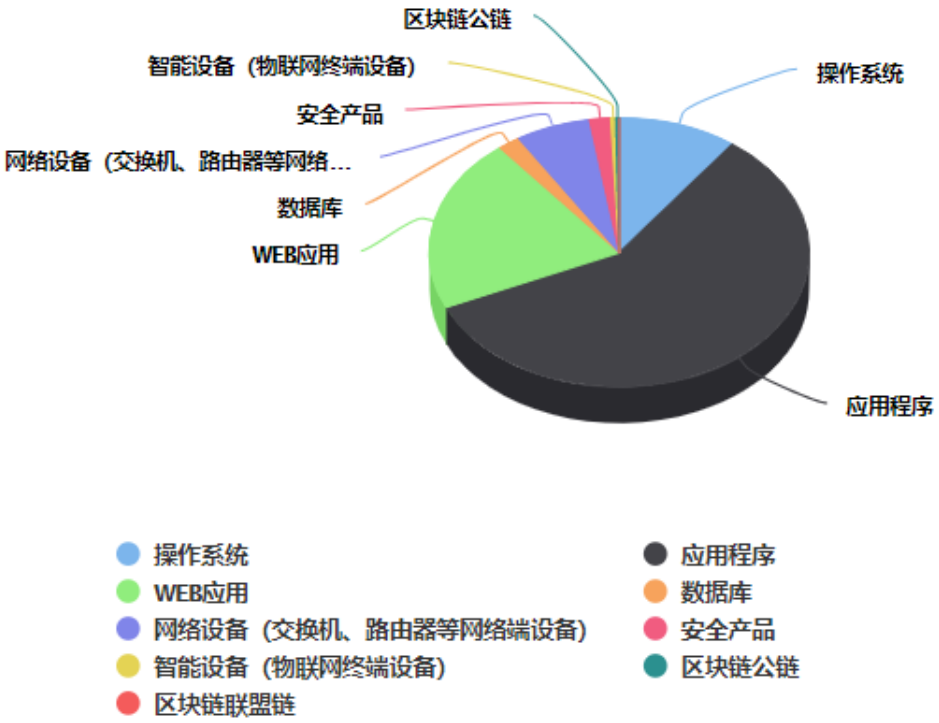
➢ **漏洞产生原因（2020 年 08 月 31 日—2020 年 09 月 13）**



➢ 漏洞引发的威胁（2020 年 08 月 31 日—2020 年 09 月 13）



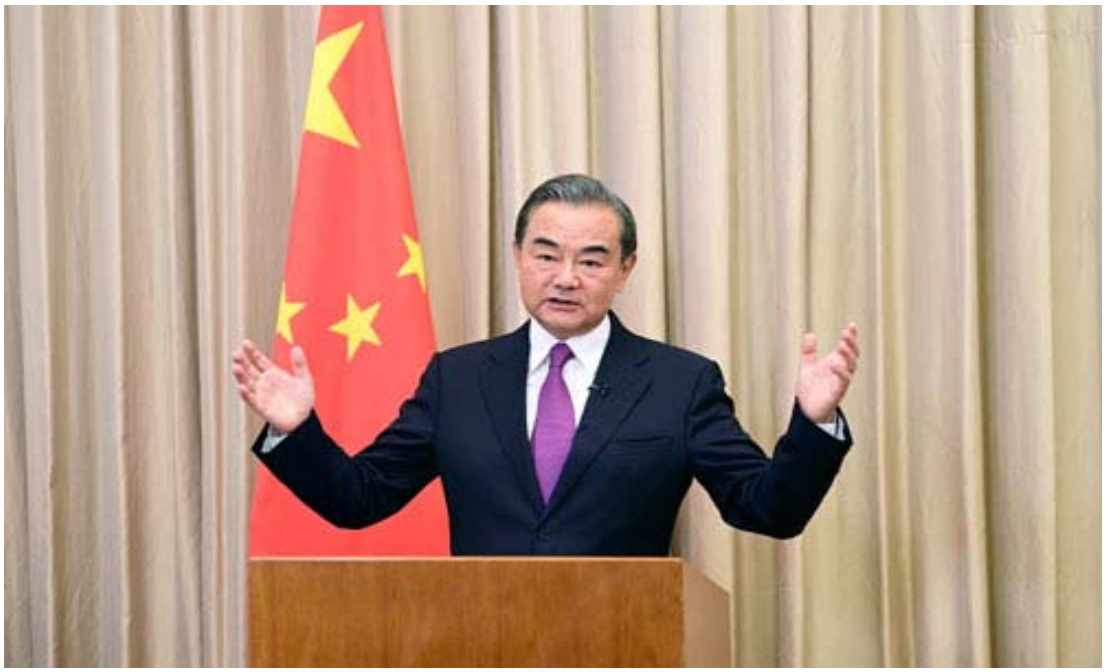
➢ 漏洞影响对象类型（2020 年 08 月 31 日—2020 年 09 月 13）



三、安全产业动态

➢ 共同构建网络空间命运共同体

“各方应在相互尊重基础上，加强沟通交流，深化对话与合作，共同构建和平、安全、开放、合作、有序的网络空间命运共同体”“我们呼吁各国支持并通过双边或地区协议等形式确认上述承诺，呼吁国际社会在普遍参与的基础上就此达成国际协议”……2020 年 9 月 8 日，中国发起《全球数据安全倡议》，提出全球数字治理应遵循的“秉持多边主义、兼顾安全发展、坚守公平正义”三原则，为全球性问题提供解决方案，体现了大国担当，符合国际社会共同期待。



共商应对数据安全风险之策，共谋全球数字治理之道，是当前国际社会面对的一大课题。最新统计显示，全球移动互联网用户已达到 35 亿，数字经济规模占全球经济总量的比重已超过 15%。作为数字技术的关键要素，全球数据爆发增长、海量集聚，如同新的“石油”，正在成为各国经济发展和产业革新的动力源泉。与此同时，攸关国家安全、公共利益和个人权利的数据安全风险，大量数据频繁跨境流动带来的治理能力考验，各国法律法规标准不一推高全球企业的合规成本，都对全球数字治理提出新的要求。

应当看到，在信息技术促动的经济全球化时代，数字技术的内在发展动力源自开放合作。秉持多边主义，在普遍参与的基础上达成反映各国意愿、尊重各方利益的全球数据安全规则是大势所趋，共商、共建、共享才是解决全球数字治理赤字的正确出路。

必须指出，维护数字安全应以事实和法规为依据，不能背弃公平正义原则。但是，美国当局最近却明目张胆地搅起一股逆流——推行所谓“清洁网络”计划，企图在国际互联网平台复制霸权战略，以“清洁”之名行“清洗”之实，打着“安全”的幌子围猎他国领先企业。这种置国际公义于不顾的“惊世”贪婪，这种人为建立数字屏障、割裂全球网络空间的疯狂霸道，严重干扰和阻碍全球数字合作与发展，着实令人愤慨。国际互联网协会日前发布声明，对美方推动所谓“清洁网络”计划并考虑推出会将互联网割裂成碎片的一系列政策深感担忧，明确指出美国政府的做法违背了互联网全球互联、开放、去中心化的本质，违背了技术架构的公平普及性。

各国都有权依法保护本国的数据安全，保护数据安全对数字经济健康发展至关重要，中方为此向全球发出具体倡议。各国应以事实为依据全面客观看待数据安全问题，积极维护全球信息技术产品和服务的供应链开放、安全、稳定。各国应反对利用信息技术破坏他国关键基础设施或窃取重要数据，以及利用其从事危害他国国家安全和社会公共利益的行为。各国应承诺采取措施防范、制止利用网络侵害个人信息的行为，反对滥用信息技术从事针对他国的大规模监控、非法采集他国公民个人信息。各国应要求企业严格遵守所在国法律，不得要求本国企业将境外产生、获取的数据存储在境内。各国应尊重他国主权、司法管辖权和对数据的安全管理权，未经他国法律允许不得直接向企业或个人调取位于他国的数据。各国如因打击犯罪等执法需要跨境调取数据，应通过司法协助渠道或其他相关多双边协议解决。国家间缔结跨境调取数据双边协议，不得侵犯第三国司法主权和数据安全。信息技术产品和服务供应企业不得在产品和服务中设置后门，非法获取用户数据、控制或操纵用户系统和设备。信息技术企业不得利用用户对产品依赖性谋取不正当利益，强迫用户升级系统或更新换代。产品供应方承诺及时向合作伙伴及用户告知产品的安全缺陷或漏洞，并提出补救措施。

网络空间是人类共同的活动空间，网络空间前途命运应由世界各国共同掌握。抓住数字机遇，共谋合作发展，是符合各国共同利益的选择。包括各国政府、企业在内的各利益攸关方理当携手努力，共同担当数字时代的全球责任，共同推进全球数字治理，共同构建网络空间命运共同体，推动实现合作共赢、共同发展。（来源：人民网）

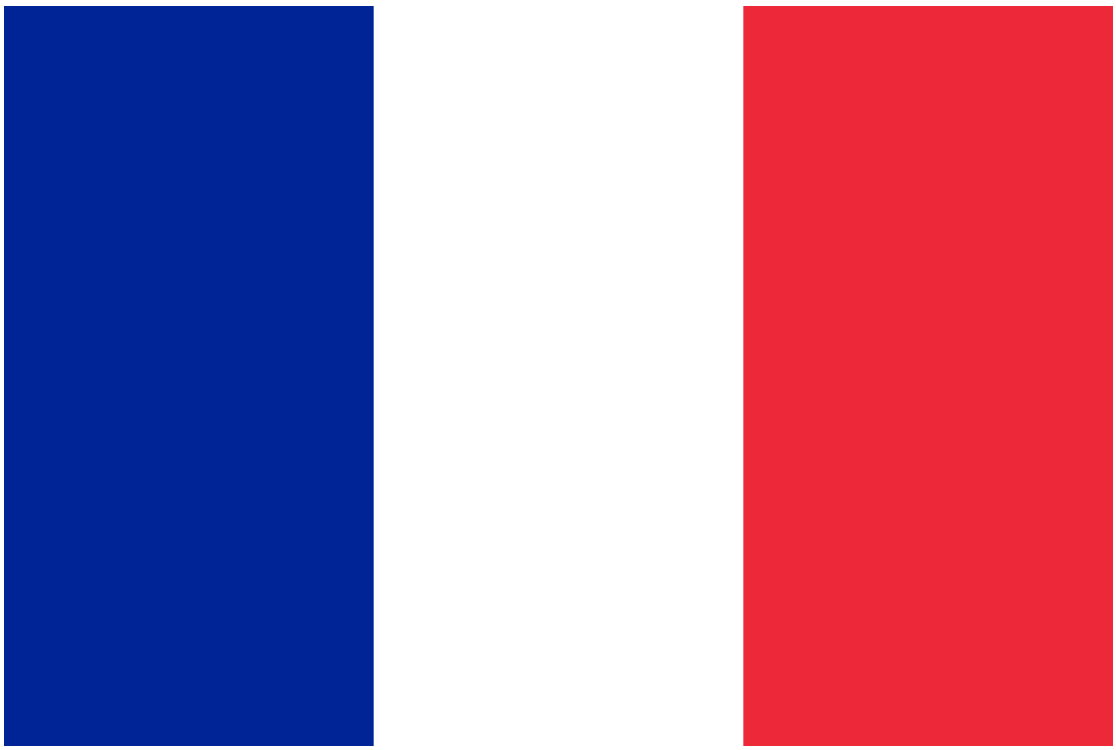
- **中华人民共和国《全球数据安全倡议》**
- **全文：**https://www.fmprc.gov.cn/web/wjbzhd/t1812949.shtml

➢ 数字时代如何保护个人信息

大数据时代，信息科技给人类社会生产生活带来诸多便利，同时也有一些烦恼随之而来。比如，骚扰电话、垃圾短信、诈骗信息等让人不胜其扰，防不胜防。身处互联网时代,如何保护个人信息安全已成为世界性难题。其他国家和地区在个人信息的立法和执行上有哪些经验和教训，今天请跟我们的驻外记者一起去看看。

法国：强化“数字主权”规避他国政策风险

早在上世纪 70 年代修改民法典时，法国就增加了“每个人都享有其隐私获得尊重的权利”的相关规定。2018 年 6 月，法国修订《信息与自由法》以匹配欧盟同年 5 月生效的《通用数据保护条例》。此外，法国《国土安全法》等诸多细分法律，对航空、媒体等领域的个人隐私信息保护进行补充规定。但近年来，空中客车公司、《费加罗报》、警察部门、外交部等多个企业、机构、机关由于人为疏忽、安全漏洞、黑客攻击等均发生过公民数据泄露情况。



这些事件的发生，首先是对隐私保护的认识与投入不足，其次就是跨国法律的矛盾。为改变这一局面，法国政府一方面下手“重罚”，另一方面则在努力摆脱他国政策带来的风险。?

2019 年 1 月，法国国家信息与自由委员会依据欧盟《通用数据保护条例》开出首个罚单，就谷歌违反数据隐私保护相关规定处以 5000 万欧元（1 欧元约合 8.20 元人民币）罚款。

今年 7 月，欧洲法院判决欧盟与美国 2016 年达成的用于跨大西洋传输个人数据的《欧美隐私盾牌》协定无效。据法国媒体报道，法国 50 余家信息技术与数据管理企业正动员起

来强化法国和欧盟的“数字主权”，法国数据管理机构建议法企业在数据存储上选择服务器设在欧洲的欧洲供应商，摆脱美国的政策风险。

俄罗斯：金融机构利用技术手段堵塞潜在泄露渠道

“售卖用户信息的行为几乎每天都在互联网上发生。”俄罗斯专门提供信息泄漏监测服务的 DeviceLock 公司创始人阿绍特·奥加涅介绍说。研究表明，在俄罗斯，公民的个人数据被盗约占客户所泄露机密信息的 77%。更糟糕的是失窃数据通常会落入不法分子手中，从而导致欺诈等行为的发生。

据俄罗斯安全公司 InfoWatch 今年 2 月发布的数据显示：2019 年俄罗斯信息泄露的记录达 270 万条，是前年的 6 倍。特别值得一提的是，2019 年全球金融机构 218 起数据泄露案件中的 33 起就发生在俄罗斯。

分析人士认为，泄露事件的大幅增加与各机构对信息保存与处理时的不负责任态度有关。金融机构客户的护照信息、电话号码和电子邮箱等占泄露信息的主体。新冠肺炎疫情使得俄罗斯个人信息泄露事件骤然增多。InfoWatch 的统计认为，这与医疗机构医疗数据受保护程度比金融机构低得多有很大关系。

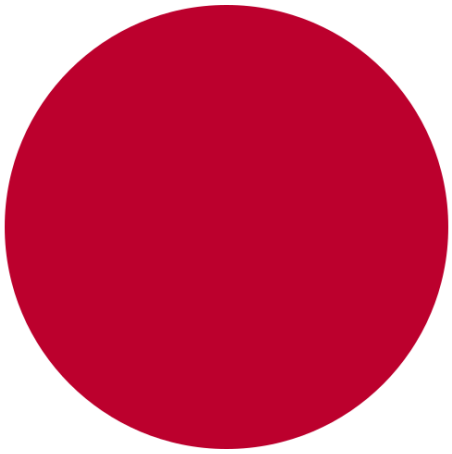
为加强个人信息保护，针对内部人员倒卖数据情况，俄罗斯外经贸银行专门划定了信息访问权，保留了具有访问权限的员工记录，并利用技术手段来控制潜在泄露渠道。

日本：修改《个人信息保护法》严格保护公民信息

尽管日本民众非常重视保护个人信息，但政府和企业因为各种原因会发生个人信息泄露

事件。

三菱电机公司 1 月 20 日发布消息称，因遭受网络攻击，导致该公司的员工、退休人员、应聘者等总计 8122 人的个人信息，以及客户相关资料及联络内容等泄露。日本经济新闻社 5 月 12 日发布消息称，该企业职工电脑感染病毒，导致公司 12514 名员工的个人信息外泄…… ？？？



日本于 2003 年制定了《个人信息保护法》，并从 2005 年 4 月 1 日开始实施。今年春天日本政府又启动修改《个人信息保护法》，以便更加严格保护个人信息。6 月 5 日，《个人信息保护法》在国会通过并成立，预计将在 2022 年 6 月前开始实施。

该法规定对使用个人数据的企业加重责任，扩大了个人权利，还把对有违规行为企业的罚金上限提升至 1 亿日元（1 元人民币约合 15.29 日元）。该法规定，在发生信息外泄时，企业有义务向个人信息保护委员会和本人报告。

比利时：建立专门执法机构保护隐私数据

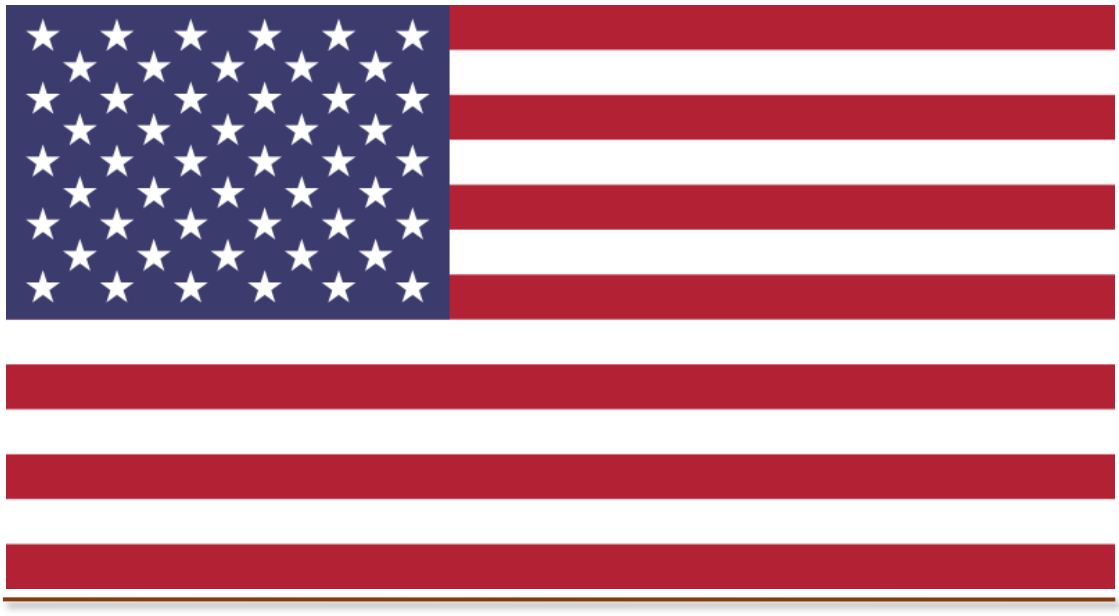
根据欧盟基本权利机构 7 月发布的报告，欧洲人目前最担心的安全问题是数据滥用、网络诈骗和恐怖主义。其中，55%的受访者担心个人在线数据被欺诈者和犯罪贩子滥用，25%的受访者担心自己的网上银行账户或银行卡被盗用。

在欧盟《通用数据保护条例》的基础上，比利时还出台了多项国家层面的相关法律。2019 年 5 月成立的比利时数据保护局是负责隐私和数据保护的执法机构，用来监督和执行对个人数据保护相关规定的遵守。

今年 7 月，比利时数据保护局对谷歌处以 60 万欧元罚款，原因是该公司侵犯网民的“被遗忘权”。据布鲁塞尔时报报道，一位比利时公众人物称与其名字相关的谷歌搜索结果中涉及毫无根据的骚扰指控，但谷歌拒绝删除这些文章。被遗忘权是欧盟《通用数据保护条例》中规定的新型权利，任何公民可以在其个人数据不再需要时提出删除要求。

比利时信息法专家蒂姆·范坎尼特指出，尽管比利时现在拥有广泛的数据保护法律框架，但在提供指导和执行方面做得还没有完全到位。范坎尼特呼吁在欧盟范围内建立真正的单一数据保护机构，以大大简化和便利工作。

美国：全面的联邦法律尚未出台



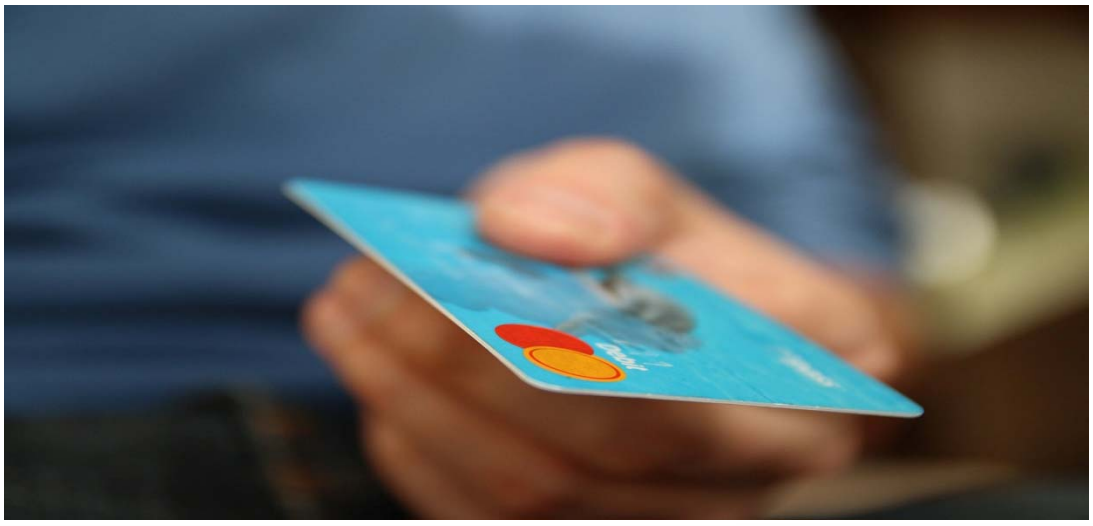
美国推特公司 8 月表示，自身可能因滥用用户个人数据而被罚款数亿美元（1 美元约合 6.91 元人民币）。在一份提交给美国证券交易委员会的材料中，该公司表示，最近已收到一份来自美国联邦贸易委员会的投诉，指责该公司从 2013 年至 2018 年间，违规将用户的电话号码、邮箱等信息用于广告目的。推特公司称，此事引发的罚款可能给公司造成 1.5 亿美元到 2.5 亿美元的损失。

近年来，已多次传出美国互联网科技企业涉及用户数据被滥用的丑闻。2018 年，脸谱公司曝出重大用户数据泄露事件，一家名为“剑桥分析”的公司被媒体曝光以不正当方式获取了超过 5000 万脸谱用户的数据，并将这些数据用于美国选举活动。同一年，谷歌公司关闭了其社交媒体业务“谷歌+”，因为谷歌在该服务中发现了一个安全漏洞，暴露了多达 50 万用户的私人数据……

《纽约时报》在评论文章中指出，美国是唯一没有全面的消费者数据保护法及相关的独立执行机构的发达国家。该文章称，美国国会从未成立一个机构来监管脸谱、优步等大规模使用个人数据的科技企业。“监管空白让美国人任由互联网服务商摆布，这些服务商有各种动机来利用我们的个人信息，却没有什么动机来保护它。”（来源：人民日报）

➢ 个人金融信息的制度保护路径

个人金融信息，又称消费者金融信息，是自然人从事金融活动产生的个人信息。在数字化时代，数据已经成为继土地、劳动力、资本、技术之后的关键生产要素，而个人金融信息是大数据时代下的重要数据来源之一，极具商业价值，往往为一些商业机构或个人所觊觎，因此导致各种风险亦层出不穷。



个人金融信息安全面临的严峻挑战

在“数据为王”的当下，各类信息中，个人金融信息的经济价值日益凸显。金融机构大量收集个人金融信息，并运用大数据、云计算等技术进行分析，描绘出包括人口统计学特征、消费能力数据、兴趣数据、风险偏好等内容的客户画像。这些举措有利于金融机构进行身份认证、精准营销、加强风险管理与控制和优化运营等，虽为金融消费者的生活带来不少便利，但同时也造成了一些人借此机会非法收集他人的个人信息、甚至是滥用和泄露个人金融信息等问题。

在 2020 年上半年，一家知名银行分支机构在未经客户授权同意的情况下，向第三方提供客户的个人银行账户交易明细，此事引发社会广泛关注。事发后，银保监会及时对该银行启动了立案调查程序，认为银行分支机构违背了为存款人保密的规定，并且严重侵害了金融消费者的信息安全保障权益。针对该银行分支机构所犯的错误，该机构很可能因此面临严厉的监管处罚。另据统计，最近几年个人金融信息泄露事件的年增长率高达 35%，这也显现出金融机构对于保障金融消费者的个人金融信息安全及相关权益面对前所未有的挑战。

个人金融信息保护的立法推进与反思

面对个人金融信息安全屡遭侵害的严峻形势，我国相继出台了众多相关法规，以此来加强对个人金融信息安全的保护。

《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》(银发〔2011〕17 号）首次明确规定了“个人金融信息”的概念及范围，并确立了个人金融信息的使用原则和基本保护框架。2015 年《刑法修正案九》将“侵犯公民个人信息罪”作为现行《刑法》第二百五十三条之一，严重侵害个人金融信息的行为会受到刑事处罚。《中国人民银行金融消

费者权益保护实施办法》（银发〔2016〕314 号）拓展了金融机构的外延，相应扩大了“个人金融信息”的范围，同时在第三章对个人金融信息保护做出专门规定。《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》（法释〔2017〕10 号）明确了“个人信息”的概念以及侵犯公民个人信息罪的具体定罪量刑标准，进一步加强了对侵害个人金融信息安全犯罪行为的打击力度。将于 2021 年实施的《民法典》，对个人信息保护做出了详细规定，从定义、处理原则、条件和免责事由，到主体权利和与之对应的信息处理者的信息安全保障义务，再到公权力机关及其工作人员的保密义务，构建了一个较为完整的个人信息保护框架。另外，2020 年 2 月央行发布了《个人金融信息保护技术规范》，为金融机构加强个人信息保护的合规建设和金融监管机构的监督、执法工作提供参考。

通过上述法律法规和规范文件可知，我国已构建了针对个人金融信息保护较详细的法律框架，但仍然存在诸多问题。

第一，个人金融信息保护的专门立法缺位，法律体系的整体协调性有所不足。我国对个人金融信息保护的法律规定比较分散，对其相关的问题缺乏统一规定，且大多数作为部门规章、规范性文件或推荐的技术标准，法律位阶和层次较低，难以满足当前金融消费者对个人金融信息安全保护的迫切需求。《民法典》与《刑法》的相关规定并非个人金融信息领域的专门立法，难以在金融机构开展具体业务及个人金融信息保护时提供有针对性的规范指导或参考依据。

第二，对于非持牌机构的金融关联业务，我国当前采取的法律规制和措施不够。相较于持牌金融机构，非持牌机构开展金融关联业务时，往往同样收集了大量个人金融相关信息，其收集范围甚至超过了必要的程度，这样就存在更多的信息安全隐患。不过，目前央行等金融监管机构已出台的法规主要针对银行、保险、证券或第三方支付等持牌金融机构，而对于涉足金融科技的非持牌机构（如移动电商与移动社交巨头）只有较少的个人金融相关信息保护的规定。

第三，针对个人金融信息的救济制度不完善。目前我国对个人金融信息的保护更侧重于行政、刑事救济，这使得权益因此受到侵犯的个人缺乏足够动力去监督、起诉违法者，从另一个方面来讲，这也负面影响到相关部门对个人金融信息的有力保护。

个人金融信息保护的路径

针对个人金融信息保护领域的严峻挑战和存在的问题，我们认为，加强个人金融信息的保护，亟待立法部门、金融机构和金融监管部门等形成多方合力，从立法、金融机构内部合规控制和监管执法三个层面进行综合考量和制度设计。

1.逐步完善个人金融信息立法。首先，要加快推动个人金融信息保护的专项立法进程，制定一部系统性的个人金融信息保护法。在具体操作层面，可借鉴当前《个人金融信息保护技术规范》，将个人金融信息按照敏感程度从高到低进行分类，针对不同级别的信息采取对应层次的更有针对性的保护措施；还可采取“分步走”的方式逐步推进，央行将《个人金融信息(数据)保护试行办法》列入 2019 年度规章制定计划当中，在落实推行该《办法》、梳理整合个人金融信息保护的相关法律规定的基础上，制定一部个人金融信息保护法，对其要素，如概念及范围、保护原则、各方主体权责、救济措施与民事赔偿等各方面加以全面规定。其次，要加强对非持牌金融业务关联机构的法律规制，将其纳入到个人金融信息保护的法律体系内。最后，要完善个人金融信息的救济机制。公法救济方面，如行政和刑事处罚，它们固然可以有力地保护个人金融信息安全，但其执法成本高，而且刑事处罚的适用条件较为严格，在大多数情况下，这并不适宜用来作为个人金融信息保护的日常救济手段。因此，完善相应的民事救济和赔偿机制便成为了相关立法的必然选择。具体来说，可以设立个人金融信息领域的过错推定责任制度、公益诉讼制度、精神损害赔偿制度，还可规定由金融机构承担有关个人金融信息泄露案件的举证责任。

2.强化金融机构的内部合规控制。据 Verizon 发布的《2019 年数据泄露调查报告》显示，36%的数据泄露是由机构内部人员造成的，因此，金融机构“内鬼”逐渐成为数据泄露的重要原因。我们认为，金融机构应重点关注以下四个方面：一是加强对相关工作人员的法规知识教育与培训，强化其对个人金融信息的安全意识。组织接触个人金融信息的员工学习关于个人信息保护的法律法规；相关人员在上岗前必须接受培训，并签署对个人金融信息保密的承诺书。二是设置接触个人金融信息的专岗和访问权限，并注重对访问的网络留痕，比如以留存访问记录的方式，对个人金融信息的接收者、变更者以及中间经手人员留下详细的数字化记录，以便为将来出现风险事件后的查询与问责提供证据。三是完善内部的监督和惩罚机制。在金融机构内部，设置个人金融信息安全监督机制，定期进行自查，及时填补危及个人金融信息安全的漏洞；对违反国家、行业和机构内部关于个人金融信息保护相关规定的人员进行严厉处罚，如予以降级或开除等；当员工严重侵害个人金融信息安全时，还应移交司法机构，追究其刑事责任。四是完善技术防护体系，提升个人金融信息的保护能力，比如设置双重密码认证、进行系统监控和实时监测等。

3.加强对个人金融信息的监管力度。信息安全权是金融消费者的一项重要权利，保护个人金融信息安全是保护金融消费者的应有之义。我们认为监管部门可从以下几点入手：第一，金融监管部门可参考《个人金融信息保护技术规范》，制定明确的个人金融信息保护的监管

标准，开展经常性的工作指导和风险提示；同时注重监管合作，破除数据壁垒，切断利用个人金融信息犯罪的产业链。第二，金融监管部门要加强对非持牌金融业务关联机构的指导和监管力度，指导其制定保护个人金融信息安全的内部管理制度；同时，由于金融风险的传导性，可考虑将其等同于持牌金融机构进行监管。第三，要严格执法，完善公示惩处机制，加大对侵害个人金融信息安全行为的打击力度，并以此来提高违法成本。第四，推动和落实金融机构对权益受到侵害的消费者的民事赔偿，激励金融消费者的外部监督作用。（来源：中央财经大学法学院　邓建鹏 周和平）

➢ 我国民法典对隐私权和个人信息的保护

现代社会中隐私权和个人信息的保护问题受到各国的高度重视。为了更好地保护广大人民群众的人格权，针对实践中隐私权与个人信息领域存在的各种突出问题，我国民法典在现行法律规定的基础上，对于隐私权和个人信息保护作出了专门规定。在民法典人格权编第六章“隐私权和个人信息保护”中，不仅对于隐私、个人信息以及个人信息的处理等基本概念作出了清晰的界定，同时明确了禁止实施的侵害隐私权的行为类型，处理个人信息应遵循的原则与合法性要件、个人信息的合理使用，还对隐私权和个人信息保护的关系问题作出了规定。在理解和适用民法典中隐私权和个人信息保护的规定方面，有以下三个问题需要重视。

一、隐私权与隐私的涵义

所谓隐私权（right to privacy）是指，自然人就其隐私所享有的不受侵害的权利，是一种

具体的人格权。民法典第一千零三十二条第一款规定：“自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。”隐私权保护的是自然人的隐私。从隐私这个词的本身就可以看出，有两方面的特点：一是“隐”，即并非公开的状态，如果已经被自然人自行公开或者合法公开的，就不是隐私；二是“私”，即私人的事情，与他人权益、公共利益等无关。正是从这两方面出发，民法典第一千零三十二条第二款将隐私界定为：“自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。”由此可见：

1.隐私仅仅是自然人所拥有的。因为保护隐私是与自然人的精神利益息息相关的，根本在于维护人格自由，保护人格尊严。也就是说，只有自然人针对隐私才享有需要法律保护的精神利益。至于法人、非法人组织并不存在隐私的问题。法人、非法人组织也存在不愿意为他人所知的活动、信息，也存在工作活动的秩序不被打扰破坏的需要，但这些要么属于国家秘密、商业秘密，要么属于生产经营秩序或者公共活动秩序的范畴。

2.我国法上的隐私被分为：私人生活安宁以及不愿为他人知晓的私密空间、私密活动、私密信息。（1）私人生活安宁，有广狭义之分，广义的私人生活安宁实际上可以涵盖私密空间、私密活动和私密信息。由于民法典第一千零三十二条第二款界定隐私时，将私人生活安宁与私密空间等并列，故此，该款中的私人生活安宁是指狭义的私人生活安宁，即自然人个人的生活不受他人非法侵扰的状态。（2）不愿为他人知晓的私密空间、私密活动、私密信息。应当说，这三者之间具有交叉重叠。因为私密空间往往进行的就是私密活动或存储私密信息，如夫妻在住宅里的夫妻性生活，个人笔记本电脑或软件程序中存储的私人日记等。但也不完全重叠，因为公共空间中也有私密活动、私密信息，例如，在餐厅大堂中，两个朋友边吃饭边聊天，这也是私密活动，不能被他人窃听或将谈话内容公开。私密空间是与公共空间相对的，民法典第一千零三十三条第二项列举了“住宅、宾馆房间”等私密空间，但不限于此，饭店、公园、银行、车站等公共场所中也存在私密空间。此外，私密空间不仅包括物理上的空间，也包括无形空间，如电子邮箱、微信群、钉钉群等，也属于私密空间。私密活动是指，自然人不愿意为他人知晓的活动，如亲友的聚餐、朋友间谈话等。

私密信息也称隐私信息。我国民法典没有采取敏感信息和非敏感信息的划分，而是将个人信息分为私密信息和非私密信息。就私密信息的认定问题，应当说，有些是没有争议的，如个人的健康信息、犯罪记录、财产状况、性取向等，肯定属于私密信息。但是，自然人的姓名、容貌、性别等，则不属于私密信息，因为这些信息尤其是姓名本来就是社会交往使用的，不可能作为私密信息。有些个人信息是否属于私密信息，存在争议，如个人在网上的读

书记录、网页浏览信息等。由于我国法上对于私密信息和非私密信息采取不同的保护方法，故此，今后司法实践中区分二者就非常重要了。笔者认为，不能应权利人单方面决定某一信息是否属于私密信息，即不能从权利人主观认识出发界定私密信息，而应当首先依据法律法规的规定加以判断，在没有规定时，则应当基于社会公众的一般认知和价值的权衡，综合考虑以下两个因素，认定某一信息是否属于私密信息：（1）该信息对于维护自然人的人身财产权益、人格尊严和人格自由的重要程度，越重要的，越可能属于私密信息；（2）该信息对于维护社会正常交往、信息自由的重要程度如何，越重要的，越不属于私密信息。

二、个人信息权益的性质

为了协调自然人的个人信息保护与信息的自由流动与利用的关系，我国民法典没有规定个人信息权，而是使用了“个人信息保护”的表述。尽管如此，从民法典对个人信息保护的相关规定可知：

首先，自然人对于个人信息享有的是民事权益而非公权利。个人信息的核心特点在于识别性，即只有能够识别特定自然人的信息才属于个人信息。这一特点决定了，保护个人信息本身不是目的，而是要防止因个人信息的处理而产生的对自然人人身财产权益乃至人格尊严、人格自由的侵害的风险。因此，从作为个人信息主体的自然人这一方来说，其主要的利益是一种防御性利益，即自然人针对个人信息享有的防止因个人信息被非法处理而致人身财产权益遭受侵害甚至人格尊严与人格自由受到侵害或损害的利益。虽然在保护个人信息问题上需要协调多方利益，包括自然人权益的保护、合理行为自由的维护、公共利益，但不能将

自然人个人信息权益的确认与围绕个人信息的各种利益的协调这两个问题对立起来。法律上对自然人个人信息权益的确认和保护本身就是对围绕着个人信息而产生的其他主体的自由或利益边界的界定。

其次，个人信息权益保护的是自然人的人格利益。民法典虽然没有规定个人信息权，但是，民法典第九百九十条第二款规定："除前款规定的人格权外，自然人享有基于人身自由、人格尊严产生的其他人格权益。"因此，可以将自然人的个人信息权益归入自然人基于人身自由、人格尊严产生的其他人格权益。民法典第一千零三十七条和第一千零二十九条对个人信息权益的具体内容作出了规定。

再次，个人信息权益可以同时保护自然人对个人信息享有的精神利益和经济利益。我国民事立法和司法实践始终坚持的是人格权一元保护模式，即通过人格权制度同时实现对精神利益和经济利益的保护。一方面，侵害个人信息权益造成财产损失的，被侵权人可依据民法典第一千一百八十二条，要求侵权人按照被侵权人的损失或者侵权人的获利赔偿；损失以及获利难以确定的，由人民法院根据实际情况确定赔偿数额。另一方面，侵害个人信息权益造成严重精神损害的，被侵权人有权依据民法典第一千一百八十三条第一款请求精神损害赔偿。因此，我国法上无须创设单独的个人信息财产权来保护自然人对个人信息的经济利益。

三、隐私权与个人信息权益的区别

隐私权和个人信息权益是我国民法典规定的两项不同的人格权益，它们都是只有自然人才能享有的人格权益。二者的密切联系表现在：私密信息既属于隐私，受到隐私权的保护，又属于个人信息，可以适用个人信息保护的法律规定。故此，民法典第一千零三十四条第二款规定："个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。"但是，隐私权和个人信息保护也有存在以下明显的区别。

1. 权益属性不同，受法律保护的强度存在差异。隐私权作为一项具体的人格权，性质上属于绝对权和支配权，具有对世效力。任何组织或个人都必须尊重隐私权，不得对之加以侵害或妨碍。个人信息权益并非具体人格权，更非绝对权和支配权，只是一种受到法律保护的人格利益。这一性质上的差异决定了二者在保护的强度和密度上存在以下差异：（1）是否适用人格权保护禁令制度不同。隐私权受到侵害时，权利人可以适用民法典第九百九十七条规定的人格权禁令制度。但是，个人信息受到侵害时，不能适用。（2）是否适用合理使用制度不同。虽然对于隐私权也有限制，但是，对于隐私权不存在合理使用的问题。因为隐私权对于自然人的人格尊严非常重要。个人信息的保护必须协调自然人权益的保护与信息自由与合理使用之间的关系。故此，依据民法典第九百九十九条，为公共利益实施新闻报道、舆论监

督等行为的，可以合理使用个人信息，同时，第一千零三十六条还专门规定了侵害个人信息的免责事由。这些规定都不适用隐私权。（3）能否规定例外的法律位阶不同。依据民法典第一千零三十三条，对于侵害隐私权的例外规定，只能由“法律”作出；而依据第一千零三十五条第一项，“法律、行政法规”就可以对处理个人信息是否需要取得自然人或者其监护人的同意作出另外的规定。

2. 能否许可他人使用即商业化利用上不同。隐私权人可以自行处分权利，如自行在网络上或向媒体公开其私密信息，但隐私是不能许可他人使用的。因为隐私权主要是消极防御的功能，不具有积极利用的权能。对于隐私的许可使用会出现违反法律、行政法规的强制性规定或者公序良俗的后果。个人信息中则可以许可他人使用。

3. 个人信息的处理规则不同。依据民法典第一千零三十三条第五项，处理他人的私密信息要么是取得隐私权人的“明确同意”，要么是依据法律的规定，否则，任何组织或者个人实施的处理他人私密信息的行为都构成侵害隐私权的行为。但是，对于处理非私密信息的个人信息，依据民法典第一千零三十五条，要么是依据法律、行政法规的规定，要么是得到该自然人或者其监护的“同意”。由此可见，民法典中私密信息和非私密的个人信息的处理规则有两点区别：其一，处理私密信息必须取得权利人的同意，而处理非私密的个人信息可以取得自然人或者其监护人的同意。也就是说，监护人也不能擅自同意他人处理被监护人的私密信息。这是因为隐私对于权利人具有更为重大的意义。其二，处理私密信息必须取得的是权利人的“明确同意”，而处理非私密的个人信息是取得自然人或者其监护人的同意。明确同意，意味着自然人不仅要依法作出了同意的意思表示，而且该同意应当是针对该私密信息被处理而单独作出的意思表示。同意，则不要求必须是单独的同意，也不要求仅针对被处理的特定个人信息作出的同意，而可以是一种概括性的同意。（来源：人民法院报）

四、政府之声

➢ 工信部《通信短信息和语音呼叫服务管理规定》公开征求意见

2020 年 8 月 31 日，工信部就《通信短信息和语音呼叫服务管理规定（征求意见稿）》公开征求意见，任何组织或个人未经用户同意或者请求，或者用户明确表示拒绝的，不得向其发送商业性短信息或拨打商业性电话。

征求意见稿提出，用户未明确同意的，视为拒绝。用户同意后又明确表示拒绝接收的，应当停止。短信息服务提供者发送端口类商业性短信的，应当确保有关用户已同意或请求接收，并保留用户同意凭证至少五个月。短信息服务提供者不得擅自改变电信网码号用途，不得将用于发送业务管理和服务类短信息的端口用于发送商业性短信息，无正当理由不得对用户接收业务管理或者服务类短信息进行限制。

基础电信业务经营者应当建立预警监测、大数据研判等机制，通过合同约定和技术手段等措施，防范未经用户同意或者请求发送的商业性短信息或拨打的商业性电话。基础电信业务经营者、移动通信转售业务经营者发现任何组织或个人违反本规定发送短信息或拨打电话的，应当采取必要措施制止其行为，可视情况限制向其提供新增通信资源或暂停相关服务。相关记录应予以保存并提供申诉途径。暂停相关服务前应告知相关方。

工业和信息化部将组织建立全国统一的“谢绝来电”平台，引导相关组织或个人尊重用户意愿规范拨打商业性电话。基础电信业务经营者应依托“谢绝来电”平台提供“谢绝来电”服务，采取便捷有效的方式登记用户关于商业性电话的接收意愿，并依据用户意愿和双方协议约定提供防侵扰服务。移动通信转售业务经营者提供“谢绝来电”服务的，参照前款规定执行。基础电信业务经营者应为移动通信转售业务经营者提供“谢绝来电”服务予以必要协

助。（来源：工业和信息化部）

- **《通信短信息和语音呼叫服务管理规定（征求意见稿）》**
- **全文：**http://www.miit.gov.cn/n1278117/n1648113/c8067062/content.html

➢ 银保监会发文规范保险公司健康管理服务 确保相关数据和信息安全

2020 年 9 月 9 日，为规范保险公司健康管理服务行为，保护消费者合法权益，银保监会日前发布《关于规范保险公司健康管理服务的通知》。近年来，越来越多的保险公司探索为客户提供健康管理服务，在提升人民群众健康水平、降低医疗费用支出等方面发挥了积极作用，但在一定程度上还存在服务质量不高、服务内容繁杂等问题。

通知明确，保险公司健康管理服务分为健康体检、健康咨询、健康促进、疾病预防、慢病管理、就医服务、康复护理等七大类型。保险公司开展健康管理服务是通过对客户健康危险因素进行干预，预防疾病发生、控制疾病发展、促进疾病康复，通过降低疾病发生率，提升健康水平，进而降低医疗费用支出。

通知要求，保险公司开展健康管理服务应遵循科学性、合理性、安全性、有效性、客观性及符合伦理学要求等基本原则，要尊重客户的知情同意权，保护客户的隐私权，确保相关数据和信息安全。银保监会有关部门负责人表示，下一步将强化健康管理服务监管，引导行业发挥优势，依法合规开展健康管理业务，促进商业健康保险稳健发展。（来源：中国银行保险监督管理委员会）

- **《中国银保监会办公厅关于规范保险公司健康管理服务的通知》全文：**
- http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=927766&itemId=928&gener

altype=0

➢ 国家市场监管总局就《商业秘密保护规定（征求意见稿）》公开征求意见

2020 年 9 月 4 日，国家市场监管总局发布《商业秘密保护规定(征求意见稿)》(下称《征求意见稿》)提出，权利人经过商业成本的付出，形成了在一定期间内相对固定的且具有独特交易习惯等内容的客户名单，可以获得商业秘密保护。

市场监管总局介绍，为加强企业商业秘密保护，制止侵犯商业秘密不正当竞争行为，激励研发与创新，优化营商环境，维护公平竞争的市场秩序，衔接《反不正当竞争法》，市场监管总局组织开展了对《关于禁止侵犯商业秘密行为的若干规定》的修订工作。意见建议反馈截止时间为 2020 年 10 月 18 日。

《征求意见稿》共六章 39 条，分为总则、商业秘密界定、侵犯商业秘密行为、对涉嫌侵犯商业秘密行为的查处、法律责任和附则。《征求意见稿》对侵犯商业秘密的行为进行细化，对以盗窃等方式非法获取商业秘密的情形、对“披露”“使用”等概念、对“保密义务或者违反权利人有关保守商业秘密要求”、对“限制性使用商业秘密”等予以细化和界定。

其中，《征求意见稿》提出，权利人经过商业成本的付出，形成了在一定期间内相对固定的且具有独特交易习惯等内容的客户名单，可以获得商业秘密保护。

客户名单一般是指客户的名称、地址、联系方式以及交易的习惯、意向、内容等构成的区别于相关公知信息的特殊客户信息，包括汇集众多客户的客户名册，以及保持长期稳定交易关系的特定客户。客户基于对职工个人的信赖而与职工所在单位进行市场交易，该职工离职后，能够证明客户自愿选择与自己或者其新单位进行市场交易的，应当认定没有采用不正

当手段。

所称权利人是指依法对商业秘密享有所有权或者使用权的自然人、法人或者非法人组织。对涉嫌侵犯商业秘密行为的查处上，《征求意见稿》增加了对权利人提交材料的要求、委托鉴定、案件中止等内容。一是明确县级以上市场监管部门对侵犯商业秘密行为进行监督检查、认定处理。二是对权利人在举报侵权行为时应当提供的证据材料予以明确。三是明确商业秘密案件引入鉴定或专家意见的情形；四是明确市场监管部门对双方当事人提供的证据材料的认定和采信规则。五是对市场监管部门对涉及侵犯商业秘密的证据进行保全的情形进行规定。六是对案件中止、司法移送、责令停止侵权等程序性内容予以细化。此外，《征求意见稿》在保留原规定关于法律责任、侵权产品处理、国家机关及其工作人员保守商业秘密的要求等内容基础上，增加了对“情节严重”认定、违法所得及造成权利人损害的计算等内容。

（来源：国家市场监管总局）

- **《商业秘密保护规定（征求意见稿）》**
- **全文：**http://www.samr.gov.cn/hd/zjdc/202009/t20200904_321386.html

➢ 公安部《落实等级保护制度和关键信息基础设施安全保护制度的指导意见》

近日，公安部公布了《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》全文，为网络运营者及关键信息基础设施运营者落实等保义务和关保义务，保护重要网络和数据安全提供了指导意见。

中华人民共和国公安部

公网安〔2020〕1960 号

关于印送《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》的函

中央和国家机关各部委，国务院各直属机构、办事机构、事业单位，各中央企业：

为深入贯彻党中央有关文件精神和《网络安全法》，指导重点行业、部门全面落实网络安全等级保护制度和关键信息基础设施安全保护制度，健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力处置重大网络安全事件，配合公安机关加强网络安全监管，严厉打击危害网络安全的违法犯罪活动，切实保障关键信息基础设施、重要网络和数据安全，公安部研究制定了《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》。现印送给你们，请结合本行业、本部门工作实际，认真参照执行。

2020 年 7 月 22 日

（联系人：张嘉斌　联系电话：010-66261662）

附：中华人民共和国公安部公网安[2020]1960号 《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》的函 全文如下：

网络安全等级保护制度和关键信息基础设施安全保护制度是党中央有关文件和《网络安全法》确定的基本制度。近年来，各单位、各部门按照中央网络安全政策要求和《网络安全法》等法律法规规定，全面加强网络安全工作，有力保障了国家关键信息基础设施、重要网络和数据安全。但随着信息技术飞速发展，网络安全工作仍面临一些新形势、新任务和新挑战。为深入贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度，健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力处置网络安全事件，严厉打击危害网络安全的违法犯罪活动，切实保障国家网络安全，特制定以下指导意见。

一、指导思想、基本原则和工作目标

（一）指导思想

以习近平新时代中国特色社会主义思想为指导，按照党中央、国务院决策部署，以总体国家安全观为统领，认真贯彻实施网络强国战略，全面加强网络安全工作统筹规划，以贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度为基础，以保护关键信息基础设施、重要网络和数据安全为重点，全面加强网络安全防范管理、监测预警、应急处置、侦查打击、情报信息等各项工作，及时监测、处置网络安全风险、威胁和网络安全突发事件，保护关键信息基础设施、重要网络和数据免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，切实提高网络安全保护能力，积极构建国家网络安全综合防控体系，切实维护国家网络空间主权、国家安全和社会公共利益，保护人民群众的合法权益，保障和促进经济社会信息化健康发展。

（二）基本原则

坚持分等级保护、突出重点。根据网络（包含网络设施、信息系统、数据资源等）在国家安全、经济建设、社会生活中的重要程度，以及其遭到破坏后的危害程度等因素，科学确定网络的安全保护等级，实施分等级保护、分等级监管，重点保障关键信息基础设施和第三级（含第三级、下同）以上网络的安全。

坚持积极防御、综合防护。按照法律法规和有关国家标准规范，充分利用人工智能、大数据分析等技术，积极落实网络安全管理和技术防范措施，强化网络安全监测、态势感知、通报预警和应急处置等重点工作，综合采取网络安全保护、保卫、保障措施，防范和遏制重大网络安全风险、事件发生，保护云计算、物联网、新型互联网、大数据、智能制造等新技术应用和新业态安全。

坚持依法保护、形成合力。依据《网络安全法》等法律法规规定，公安机关依法履行网络安全保卫和监督管理职责，网络安全行业主管部门（含监管部门，下同）依法履行本行业网络安全主管、监管责任，强化和落实网络运营者主体防护责任，充分发挥和调动社会各方力量，协调配合、群策群力，形成网络安全保护工作合力。

（三）工作目标

网络安全等级保护制度深入贯彻实施。网络安全等级保护定级备案、等级测评、安全建设和检查等基础工作深入推进。网络安全保护“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施得到有效落实，网络安全保护良好生态基本建立，国家网络安全综合防护能力和水平显著提升。

关键信息基础设施安全保护制度建立实施。关键信息基础设施底数清晰，安全保护机构健全、职责明确、保障有力。在贯彻落实网络安全等级保护制度的基础上，关键信息基础设施涉及的关键岗位人员管理、供应链安全、数据安全、应急处置等重点安全保护措施得到有效落实，关键信息基础设施安全防护能力明显增强。

网络安全监测预警和应急处置能力显著提升。跨行业、跨部门、跨地区的立体化网络安全监测体系和网络安全保护平台基本建成，网络安全态势感知、通报预警和事件发现处置能力明显提高。网络安全预案科学齐备，应急处置机制完善，应急演练常态化开展，网络安全重大事件得到有效防范、遏制和处置。

网络安全综合防控体系基本形成。网络安全保护工作机制健全完善，党委统筹领导、各部门分工负责、社会力量多方参与的网络安全工作格局进一步完善。网络安全责任制得到有效落实，网络安全管理防范、监督指导和侦查打击等能力显著提升，“打防管控”一体化的网络安全综合防控体系基本形成。

二、深入贯彻实施国家网络安全等级保护制度

按照国家网络安全等级保护制度要求，各单位、各部门在公安机关指导监督下，认真组织、深入开展网络安全等级保护工作，建立良好的网络安全保护生态，切实履行主体责任，全面提升网络安全保护能力。

（一）深化网络定级备案工作。网络运营者应全面梳理本单位各类网络，特别是云计算、物联网、新型互联网、大数据、智能制造等新技术应用的基本情况，并根据网络的功能、服务范围、服务对象和处理数据等情况，科学确定网络的安全保护等级，对第二级以上网络依法向公安机关备案，并向行业主管部门报备。对新建网络，应在规划设计阶段确定安全保护等级。公安机关对网络运营者提交的备案材料和网络的安全保护等级进行审核，对定级结果

合理、备案材料符合要求的，及时出具网络安全等级保护备案证明。行业主管部门可以依据《网络安全等级保护定级指南》国家标准，结合行业特点制定行业网络安全等级保护定级指导意见。

（二）定期开展网络安全等级测评。网络运营者应依据有关标准规范，对已定级备案网络的安全性进行检测评估，查找可能存在的网络安全问题和隐患。第三级以上网络运营者应委托符合国家有关规定的等级测评机构，每年开展一次网络安全等级测评，并及时将等级测评报告提交受理备案的公安机关和行业主管部门。新建第三级以上网络应在通过等级测评后投入运行。网络运营者在开展测评服务过程中要与测评机构签署安全保密协议，并对测评过程进行监督管理。公安机关要加强对本地等级测评机构的监督管理，建立测评人员背景审查和人员审核制度，确保等级测评过程客观、公正、安全。

（三）科学开展安全建设整改。网络运营者应在网络建设和运营过程中，同步规划、同步建设、同步使用有关网络安全保护措施。应依据《网络安全等级保护基本要求》《网络安全等级保护安全设计技术要求》等国家标准，在现有安全保护措施的基础上，全面梳理分析安全保护需求，并结合等级测评过程中发现的问题隐患，按照“一个中心（安全管理中心）、三重防护（安全通信网络、安全区域边界、安全计算环境）”的要求，认真开展网络安全建设和整改加固，全面落实安全保护技术措施。网络运营者可将网络迁移上云，或将网络安全服务外包，充分利用云服务商和网络安全服务商提升网络安全保护能力和水平。应全面加强网络安全管理，建立完善人员管理、教育培训、系统安全建设和运维等管理制度，加强机房、设备和介质安全管理，强化重要数据和个人信息保护，制定操作规范和工作流程，加强日常监督和考核，确保各项管理措施有效落实。

（四）强化安全责任落实。行业主管部门、网络运营者应依据《网络安全法》等法律法规和有关政策要求，按照“谁主管谁负责、谁运营谁负责”的原则，厘清网络安全保护边界，明确安全保护工作责任，建立网络安全等级保护工作责任制，落实责任追究制度，作到“守土有责、守土尽责”。网络运营者要定期组织专门力量开展网络安全自查和检测评估，行业主管部门要组织风险评估，及时发现网络安全隐患和薄弱环节并予以整改，不断提高网络安全保护能力和水平。

（五）加强供应链安全管理。网络运营者应加强网络关键人员的安全管理，第三级以上网络运营者应对为其提供设计、建设、运维、技术服务的机构和人员加强管理，评估服务过程中可能存在的安全风险，并采取相应的管控措施。网络运营者应加强网络运维管理，因业务需要确需通过互联网远程运维的，应进行评估论证，并采取相应的管控措施。网络运营者

应采购、使用符合国家法律法规和有关标准规范要求的网络产品及服务，第三级以上网络运营者应积极应用安全可信的网络产品及服务。

（六）落实密码安全防护要求。网络运营者应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。

三、建立并实施关键信息基础设施安全保护制度

公安机关指导监督关键信息基础设施安全保护工作。各单位、各部门应加强关键信息基础设施安全的法律体系、政策体系、标准体系、保护体系、保卫体系和保障体系建设，建立并实施关键信息基础设施安全保护制度，在落实网络安全等级保护制度基础上，突出保护重点，强化保护措施，切实维护关键信息基础设施安全。

（一）组织认定关键信息基础设施。根据党中央和公安部有关规定，公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的主管、监管部门（以下统称保护工作部门）应制定本行业、本领域关键信息基础设施认定规则并报公安部备案。保护工作部门根据认定规则负责组织认定本行业、本领域关键信息基础设施，及时将认定结果通知相关设施运营者并报公安部。应将符合认定条件的基础网络、大型专网、核心业务系统、云平台、大数据平台、物联网、工业控制系统、智能制造系统、新型互联网、新兴通讯设施等重点保护对象纳入关键信息基础设施。关键信息基础设施清单实行动态调整机制，有关网络设施、信息系统发生较大变化，可能影响其认定结果的，运营者应及时将相关情况报告保护工作部门，保护工作部门应组织重新认定，将认定结果通知运营者，并报公安部。

（二）明确关键信息基础设施安全保护工作职能分工。公安部负责关键信息基础设施安全保护工作的顶层设计和规划部署，会同相关部门健全完善关键信息基础设施安全保护制度体系。保护工作部门负责对本行业、本领域关键信息基础设施安全保护工作的组织领导，根据国家网络安全法律法规和有关标准规范要求，制定并实施本行业、本领域关键信息基础设施安全总体规划和安全防护策略，落实本行业、本领域网络安全指导监督责任。关键信息基础设施运营者负责设置专门安全管理机构，组织开展关键信息基础设施安全保护工作，主要负责人对本单位关键信息基础设施安全保护负总责。

（三）落实关键信息基础设施重点防护措施。关键信息基础设施运营者应依据网络安全

等级保护标准开展安全建设并进行等级测评，发现问题和风险隐患要及时整改；依据关键信息基础设施安全保护标准，加强安全保护和保障，并进行安全检测评估。要梳理网络资产，建立资产档案，强化核心岗位人员管理、整体防护、监测预警、应急处置、数据保护等重点保护措施，合理分区分域，收敛互联网暴露面，加强网络攻击威胁管控，强化纵深防御，积极利用新技术开展网络安全保护，构建以密码技术、可信计算、人工智能、大数据分析等为核心的网络安全保护体系，不断提升关键信息基础设施内生安全、主动免疫和主动防御能力。有条件的运营者应组建自己的安全服务机构，承担关键信息基础设施安全保护任务，也可通过迁移上云或购买安全服务等方式，提高网络安全专业化、集约化保障能力。

（四）加强重要数据和个人信息保护。运营者应建立并落实重要数据和个人信息安全保护制度，对关键信息基础设施中的重要网络和数据库进行容灾备份，采取身份鉴别、访问控制、密码保护、安全审计、安全隔离、可信验证等关键技术措施，切实保护重要数据全生命周期安全。运营者在境内运营中收集和产生的个人信息和重要数据应当在境内存储，因业务需要，确需向境外提供的，应当遵守有关规定并进行安全评估。

（五）强化核心岗位人员和产品服务的安全管理。要对专门安全管理机构的负责人和关键岗位人员进行安全背景审查，加强管理。要对关键信息基础设施设计、建设、运行、维护等服务实施安全管理，采购安全可信的网络产品和服务，确保供应链安全。当采购产品和服务可能影响国家安全的，应按照国家有关规定通过安全审查。公安机关加强对关键信息基础设施安全服务机构的安全管理，为运营者开展安全保护工作提供支持。

四、加强网络安全保护工作协作配合

行业主管部门、网络运营者与公安机关要密切协同，大力开展安全监测、通报预警、应急处置、威胁情报等工作，落实常态化措施，提升应对、处置网络安全突发事件和重大风险防控能力。

（一）加强网络安全立体化监测体系建设。各单位、各部门要全面加强网络安全监测，对关键信息基础设施、重要网络等开展实时监测，发现网络攻击和安全威胁，立即报告公安机关和有关部门并采取有效措施处置。要加强网络新技术研究和应用，研究绘制网络空间地理信息图谱（网络地图），实现挂图作战。行业主管部门、网络运营要建设本行业、本单位的网络安全保护业务平台，建设平台智慧大脑，依托平台和大数据开展实时监测、通报预警、应急处置、安全防护、指挥调度等工作，并与公安机关有关安全保卫平台对接，形成条块结合、纵横联通、协同联动的综合防控大格局。重点行业、网络运营者和公安机关要建设网络安全监控指挥中心，落实7x24小时值班值守制度，建立常态化、实战化的网络安全工作机

制。

（二）加强网络安全信息共享和通报预警。行业主管部门、网络运营者要依托国家网络与信息安全信息通报机制，加强本行业、本领域网络安全信息通报预警力量建设，及时收集、汇总、分析各方网络安全信息，加强威胁情报工作，组织开展网络安全威胁分析和态势研判，及时通报预警和处置。第三级以上网络运营者和关键信息基础设施运营者要开展网络安全监测预警和信息通报工作，及时接收、处置来自国家、行业和地方网络安全预警通报信息，按规定向行业主管部门、备案公安机关报送网络安全监测预警信息和网络安全事件。公安机关要加强网络与信息安全信息通报预警机制建设和力量建设，不断提高网络安全通报预警能力。

（三）加强网络安全应急处置机制建设。行业主管部门、网络运营者要按照国家有关要求制定网络安全应急预案，加强网络安全应急力量建设和应急资源储备，与公安机关密切配合，建立网络安全事件报告制度和应急处置机制。关键信息基础设施运营者和第三级以上网络运营者应定期开展应急演练，有效处置网络安全事件，并针对应急演练中发现的突出问题和漏洞隐患，及时整改加固，完善保护措施。行业主管部门、网络运营者应配合公安机关每年组织开展的网络安全监督检查、比武演习等工作，不断提升安全保护能力和对抗能力。

（四）加强网络安全事件处置和案件侦办。关键信息基础设施、第三级以上网络发生重大网络安全威胁和事件时，行业主管部门、网络运营者和公安机关应联合开展处置。电信业务经营者、网络服务提供者应提供支持及协助。网络运营者应配合公安机关打击网络违法犯罪活动；发现违法犯罪线索、重大网络安全威胁和事件时，应及时报告公安机关和有关部门并提供必要协助。

（五）加强网络安全问题隐患整改督办。公安机关建立挂牌督办制度，针对网络运营者网络安全工作不力、重大安全问题隐患久拖不改，或存在较大网络安全风险、发生重大网络安全案事件的，按照规定的权限和程序，会同行业主管部门对相关负责人进行约谈，挂牌督办，并加大监督检查和行政执法力度，依法依规进行行政处罚。网络运营者应按照有关要求采取措施，及时进行整改，消除重大风险隐患。发生重大网络安全案事件的，行业主管部门应组织全行业开展整改整顿。

五、加强网络安全工作各项保障

（一）加强组织领导。各单位、各部门要高度重视网络安全等级保护和关键信息基础设施安全保护工作，将其列入重要议事日程，加强统筹领导和规划设计，认真研究解决网络安全机构设置、人员配备、经费投入、安全保护措施建设等重大问题。行业主管部门和网络运

营者要明确本单位主要负责人是网络安全的第一责任人，并确定一名领导班子成员分管网络安全工作，成立网络安全专门机构，明确任务分工，一级抓一级，层层抓落实。

（二）加强经费政策保障。各单位、各部门要通过现有经费渠道、保障关键信息基础设施、第三级以上网络等开展等级测评、风险评估、密码应用安全性检测、演练竞赛、安全建设整改、安全保护平台建设、密码保障系统建设、运行维护、监督检查、教育培训等经费投入。关键信息基础设施运营者应保障足额的网络安全投入，作出网络安全和信息化有关决策时应有网络安全管理机构人员参与。有关部门要扶持重点网络安全技术产业和项目，支持网络安全技术研究开发和创新应用，推动网络安全产业健康发展。公安机关要会同相关部门组织实施“一带一路”网络安全战略，支持网络安全企业“走出去”， 与有关国家共享中国网络安全保护经验。

（三）加强考核评价。各单位、各部门要进一步健全完善网络安全考核评价制度，明确考核指标，组织开展考核。公安机关将网络安全工作纳入社会治安综合治理考核评价体系，每年组织对各地区网络安全工作进行考核评价，每年评选网络安全等级保护、关键信息基础设施安全保护工作先进单位，并将结果报告党委政府，通报网信部门。

（四）加强技术攻关。各单位、各部门要充分调动网络安全企业、科研机构、专家等社会力量积极参与网络安全核心技术攻关，加强网络安全协同协作、互动互补、共治共享和群防群治。公安机关要会同有关部门加强网络安全等级保护和关键信息基础设施安全保护标准制定工作，出台标准应用指南，加强标准宣贯和应用实施，建设试点示范基地，促进我国网络安全产业和企业的健康发展。

（五）加强人才培养。各单位、各部门要加强网络安全等级保护和关键信息基础设施安全保护业务交流，通过组织开展比武竞赛等形式，发现选拔高精尖技术人才，建设人才库，建立健全人才发现、培养、选拔和使用机制，为做好网络安全工作提供人才保障。（来源：公安部）

五、本期重要漏洞实例

➢ Microsoft 发布 2020 年 9 月安全更新

发布日期：2020-09-11

更新日期：2020-09-11

9 月 8 日，微软发布了 2020 年 9 月份的月度例行安全公告，修复了其多款产品存在的 125 个安全漏洞。受影响的产品包括：Windows 10 2004 & WindowsServer v2004（77 个）、Windows 10 1909 & WindowsServer v1909（75 个）、Windows 10 1903 & WindowsServer v1903（76 个）、Windows 8.1 & Server 2012 R2（47 个）、Windows RT 8.1（41 个）、Windows Server 2012（45 个）、Microsoft Edge (EdgeHTML-based)（4 个）、Internet Explorer（4 个）和 Microsoft Office-related software（23 个）。利用上述漏洞，攻击者可以提升权限，绕过安全功能限制，获取敏感信息，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	公告标题和摘要	最高严重等级和漏洞影响	受影响的软件
CVE-2020-0718	**Active Directory 远程代码执行漏洞** 当 Active Directory integrated DNS (ADIDNS) 错误处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的经过身份验证的攻击者可以在本地系统帐户的上下文中运行任意代码。 要利用此漏洞进行攻击，经过身份验证的攻击者可以向 Active Directory integrated DNS (ADIDNS) 服务器发送恶意请求。 此更新通过更正 Active Directory integrated DNS (ADIDNS) 处理内存中对象的方式来解决此漏洞。	重要 远程代码执行	Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Server 2012 Server 2012 R2
CVE-2020-0922	**Microsoft COM for Windows 远程代码执行漏洞** Microsoft COM for Windows 处理内存中的对象存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在目标系统上执行任意代码。 要利用此漏洞，用户必须打开特制文件或将目标引诱到托管恶意 JavaScript 的网站。 该安全更新通过更正 Microsoft COM for Windows 处理内存中对象的方式来解决此漏洞。	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1129	**Microsoft Windows Codecs Library 远程执行代码漏洞** Microsoft Windows Codecs Library 处理内存中的对象存在远程代码执行漏洞。成功利用此漏洞的攻击者可以获取信息，以进一步危害用户的系统。 利用此漏洞需要程序处理经特殊设计的图像文件。	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004

	此更新通过更正 Microsoft Windows Codecs Library 如何处理内存中的对象来解决漏洞。		
CVE-2020-1319	**Microsoft Windows Codecs Library 远程代码执行漏洞** Microsoft Windows Codecs Library 处理内存中的对象存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序。查看，更改或删除数据；或创建具有完全用户权限的新帐户。 利用此漏洞需要程序处理经特殊设计的图像文件。 此更新通过更正 Microsoft Windows Codecs Library 如何处理内存中的对象来解决漏洞。	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-0908	**Windows Text Service 模块远程执行代码漏洞** 当 Windows Text Service 模块未能正确处理内存时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者系统上执行。 攻击者可通过 Microsoft Edge（基于 Chromium）利用该漏洞的特制网站，然后诱使用户查看该网站。攻击者还可以通过添加可以利用此漏洞的特殊设计的内容，来利用受感染的网站以及接受或托管用户提供的内容或广告的网站。在所有情况下，攻击者都无法强迫用户查看攻击者控制的内容。相反，攻击者必须诱使用户采取措施，通常是通过诱使电子邮件或 Instant Messenger 消息，或者诱使用户打开通过电子邮件发送的附件。 该安全更新通过更正 Windows Text Service 模块处理内存的方式来解决漏洞。	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004
CVE-2020-1285	**GDI +远程代码执行漏洞** Windows Graphics Device Interface (GDI) 处理内存中的对象存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可能会安装程序。查看，更改或删除数据；或创建具有完全用户权限的新帐户。与使用管理用户权限进行操作的用户相比，将其帐户配置为在系统上具有较少用户权限的用户受到的影响较小。 该安全更新通过更正 Windows GDI 处理内存中对象的方式来解决漏洞。	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1508	**Windows Media Audio Decoder 远程代码执行漏洞** 当 Windows Media Audio Decoder 未能正确地处理对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。 攻击者可以通过多种方式利用此漏洞，例如说服用户打开构建的文档，或说服用户访问恶意网页。 安全更新通过更正 Windows Media Audio Decoder 处理对象的方式来解决该漏洞。	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2

CVE-2020-0836	**Windows DNS 拒绝服务漏洞** Windows DNS 未能正确处理查询时，存在拒绝服务漏洞。成功利用此漏洞的攻击者可能导致 DNS 服务无响应。 为了利用此漏洞，经过身份验证的攻击者可以将恶意 DNS 查询发送到目标，从而导致拒绝服务。 此更新通过更正 Windows DNS 处理查询的方式来解决漏洞。	重要 拒绝服务	Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Server 2012 Server 2012 R2
CVE-2020-1012	**WinINet API 提升权限漏洞** Wininit.dll 处理内存中的对象存在权限提升漏洞。成功利用此漏洞的攻击者可以以提升的权限执行代码。 该安全更新通过确保 Wininit.dll 正确处理内存中的对象来解决此漏洞。	重要 特权提升	Internet Explorer 11
CVE-2020-0878	**Microsoft Browser 内存破坏漏洞** Microsoft browsers 访问内存中对象的方式中存在远程代码执行漏洞。该漏洞可能以一种允许攻击者在当前用户的上下文中执行任意代码的方式来破坏内存。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，则攻击者可以控制受影响的系统。然后，攻击者可能会安装程序。查看，更改或删除数据；或创建具有完全用户权限的新帐户。 攻击者可通过 Microsoft browsers 利用此漏洞的特制网站，然后诱使用户查看该网站。攻击者还可以通过添加可以利用此漏洞的经特殊设计的内容，来利用受感染的网站或接受或托管用户提供的内容或广告的网站。在所有情况下，攻击者都无法强迫用户查看攻击者控制的内容。相反，攻击者必须说服用户采取措施，通常是通过诱使电子邮件或即时消息，或者诱使用户打开电子邮件附件。 该安全更新通过修改 Microsoft browsers 处理内存中对象的方式来解决此漏洞。	严重 远程代码执行	Internet Explorer 11 Internet Explorer 9 Microsoft Edge(Edge HTML-based) ChakraCore
CVE-2020-16884	**Internet Explorer Browser Helper Object (BHO) 内存破坏漏洞** Internet Explorer 上的 IEToEdge Browser Helper Object (BHO)插件处理内存中的对象的方式存在远程代码执行漏洞。该漏洞可能以一种攻击者可以在当前用户的上下文中执行任意代码的方式来破坏内存。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。 在基于 Web 的攻击情形中，攻击者可利用此漏洞的特制网站，然后诱使用户查看该网站。攻击者无法强迫用户查看攻击者控制的内容。相反，攻击者必须说服用户采取措施，通常是让用户单击电子邮件或 Instant Messenger 消息中的链接（将用户带到攻击者的网站），或者打开通过电子邮件发送的附件。如果当前用户使用管理用户权限登录，则成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可	重要 远程代码执行	Internet Explorer 11 Microsoft Edge (Chromium based)

	以安装程序。查看，更改或删除数据；或创建具有完全用户权限的新帐户。 该安全更新通过修改 IEToEdge BHO 插件处理内存中对象的方式来解决该漏洞。		
CVE-2020-1210	**Microsoft SharePoint 远程代码执行漏洞** 当软件未能检查应用程序包的源标记时，Microsoft SharePoint 存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在 SharePoint 应用程序池和 SharePoint 服务器场帐户的上下文中运行任意代码。 要利用此漏洞，需要用户将特制的 SharePoint 应用程序包上传到受影响的 SharePoint 版本。 该安全更新通过更正 SharePoint 如何检查应用程序包的源标记的方式来解决漏洞。	严重 远程代码执行	SharePoint Server 2010 SharePoint Enterprise Server 2013 SharePoint Enterprise Server 2016 SharePoint Server 2019 Business Prod Servers 2010
CVE-2020-1595	**Microsoft SharePoint 远程代码执行漏洞** Microsoft SharePoint 存远程代码执行漏洞，在该漏洞中，未能正确保护 API 免受不安全数据输入的攻击。成功利用此漏洞的攻击者可以在 SharePoint 应用程序池和 SharePoint 服务器场帐户的上下文中运行任意代码。 利用此漏洞要求用户使用特殊格式的输入在受影响的 SharePoint 版本上访问易受感染的 API。 该安全更新通过更正 SharePoint 处理不信任数据的反序列化的方式来解决此漏洞。	严重 远程代码执行	SharePoint Foundation 2013 SharePoint Enterprise Server 2013 SharePoint Enterprise Server 2016 SharePoint Server 2019
CVE-2020-1218	**Microsoft Word 远程代码执行漏洞** 当 Microsoft Word 软件未能正确处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以使用特制文件在当前用户的安全上下文中执行操作。例如，文件然后可以代表登录用户执行与当前用户相同的权限来执行操作。 要利用此漏洞，用户必须使用受影响的 Microsoft Word 软件版本打开特制文件。在电子邮件攻击情形中，攻击者可以通过将特制文件发送给用户并说服用户打开文件来利用此漏洞。在基于 Web 的攻击情形中，攻击者可能拥有一个网站（或利用受感染的网站来接受或托管用户提供的内容），该网站包含旨在利用此漏洞的特制文件。攻击者无法强迫用户访问该网站。相反，攻击者必须诱使用户单击链接（通常是通过诱使电子邮件或 Instant Messenger 消息的方式），然后诱使用户打开特制文件。 该安全更新通过更正 Microsoft Word 处理内存中文件的方式来解决此漏洞。	重要 远程代码执行	Word 2010/2013/2016 Office 2010 Office 2019 365 Apps Enterprise SharePoint Server 2010 SharePoint Enterprise Server 2013 SharePoint Enterprise Server 2016 SharePoint Server 2019 Office Online Server Office Web Apps 2010 Office 2016/2019 for Mac
CVE-2020-1335	**Microsoft Excel 远程代码执行漏洞** 当 Microsoft Excel 软件未能正确处理内存中的对象时，该软件中存在远程代码执行漏洞。成功利用此漏洞的攻击者可	重要 远程代码执行	Excel 2010/2013/2016 Office 2010/2013/2016/2019

	以在当前用户的上下文中运行任意代码。如果当前用户使用管理用户权限登录，攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。与使用管理用户权限操作的用户相比，帐户配置为在系统上具有较少用户权限的用户受到的影响较小。 利用此漏洞需要用户使用受影响的 Microsoft Excel 版本打开构建的文件。在电子邮件攻击场景中，攻击者可以通过向用户发送构建的文件并说服用户打开该文件来利用该漏洞进行攻击。在基于 web 的攻击场景中，攻击者可以托管一个网站（或利用接受或托管用户提供内容的受损网站），该网站包含精心编制的文件，旨在利用此漏洞进行攻击。攻击者无法强迫用户访问该网站。相反，攻击者必须说服用户单击链接，通常是通过电子邮件或即时消息中的诱惑，然后说服用户打开精心编制的文件。 安全更新通过更正 Microsoft Excel 如何处理内存中的对象来解决该漏洞。		365 Apps Enterprise SharePoint Server 2019 Office Online Server

参考信息

- https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Sep
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/adv990001

➢ Cisco NX-OS 拒绝服务漏洞

发布日期：2020-09-2
更新日期：2020-09-2
受影响系统：
Cisco Cisco NX-OS
描述：

CVE(CAN) ID: CVE-2020-3338
Cisco NX-OS 是适用于 Cisco Nexus 系列以太网交换机和 MDS 系列光纤通道存储区域网络交换机的网络操作系统。Cisco NX-OS 的 IPv6 网络（PIM6）的协议无关组播（PIM）功能存在拒绝服务漏洞。该漏洞源于在处理入站 PIM6 数据包时错误处理不当。远程未认证攻击者可通过发送多个特制 PIM6 数据包利用该漏洞导致拒绝服务。
建议：

厂商补丁：
Cisco
厂商已发布了漏洞修复程序，请及时关注更新：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-pim-memleak-dos-tC8eP7uw

➢ IBM Security Guardium Data Encryption (GDE)硬编码凭据漏洞

发布日期：2020-09-2
更新日期：2020-09-2
受影响系统：
IBM Security Guardium Data Encryption (GDE) 3.0.0.2
描述：

CVE(CAN) ID: CVE-2019-4694
IBM Security Guardium Data Encryption (GDE)提供了一组模块化的加密解决方案，可帮助安全团队有效地实现整个组织的静态数据安全性。IBM Security Guardium Data Encryption (GDE) 3.0.0.2 存在硬编码凭据漏洞，攻击者可利用该漏洞获取密码、加密密钥等硬编码凭据。
建议：

厂商补丁：
IBM
厂商已发布了漏洞修复程序，请及时关注更新：
https://www.ibm.com/support/pages/node/6320835

➢ Citrix Systems XenMobile Server 访问控制错误漏洞

发布日期：2020-08-31
更新日期：2020-08-31
受影响系统：
Citrix Systems XenMobile Server <10.12 RP3
Citrix Systems XenMobile Server <10.11 RP6
Citrix Systems XenMobile Server <10.10 RP6
Citrix Systems XenMobile Server <10.9 RP5
描述：

CVE(CAN) ID: CVE-2020-8212
Citrix Systems XenMobile Server 是美国思杰系统（Citrix Systems）公司的一套移动管理解决方案。该方案能够管理移动设备、制定移动策略和合规性规则、深入了解移动移动网络运行情况等。Citrix Systems XenMobile Server 中存在安全漏洞，该漏洞源于访问控制不当。攻击者可利用该漏洞访问权限较高的功能。
建议：

厂商补丁：
Citrix Systems
厂商已发布了漏洞修复程序，请及时关注更新：
https://support.citrix.com/article/CTX277457

六、本期网络安全事件

➢ 思科前员工离职后删库 直接损失达 240 万美元

2020 年 8 月 26 日，美国检察官办公室和联邦调查局发布公告，称思科前员工 Sudhish Kasaba Ramesh 当日在圣何塞联邦法院认罪，承认自己非法入侵思科公司的云基础设施，并破坏大量资源，造成难以挽回的损失。Sudhish Kasaba Ramesh 曾于 2016 年 7 月至 2018 年 4 月供职于思科。

United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
NORTHERN DISTRICT of CALIFORNIA

HOME ABOUT NEWS U.S. ATTORNEY NOTIFICATIONS PROGRAMS FAQ CONTACT

U.S. Attorneys » Northern District of California » News

Department of Justice

U.S. Attorney's Office

Northern District of California

SHARE

FOR IMMEDIATE RELEASE — Wednesday, August 26, 2020

San Jose Man Pleads Guilty To Damaging Cisco's Network

Unauthorized Access Led to Deletion of 16,000 WebEx Teams Accounts in the Fall of 2018

SAN JOSE – Sudhish Kasaba Ramesh pleaded guilty in federal court in San Jose today to intentionally accessing a protected computer without authorization and recklessly causing damage, announced United States Attorney David L. Anderson and Federal Bureau of Investigation Special Agent in Charge John L. Bennett.

According to the plea agreement, Ramesh admitted to intentionally accessing Cisco Systems' cloud infrastructure that was hosted by Amazon Web Services without Cisco's permission on September 24, 2018. Ramesh worked for Cisco and resigned in approximately April 2018. During his unauthorized access, Ramesh admitted that he deployed a code from his Google Cloud Project account that resulted in the deletion of 456 virtual machines for Cisco's WebEx Teams application, which provided video meetings, video messaging, file sharing, and other collaboration tools. He further admitted that he acted recklessly in deploying the code, and consciously disregarded the substantial risk that his conduct could harm to Cisco. As a result of Ramesh's conduct, over 16,000 WebEx Teams accounts were shut down for up to two weeks, and caused Cisco to spend approximately $1,400,000 in employee time to restore the damage to the application and refund over $1,000,000 to affected customers. No customer data was compromised as a result of the defendant's conduct.

恶意删除思科四百多台虚拟机的 Sudhish Kasaba Ramesh 在 2016 年 7 月到 2018 年 4 月

期间在思科任职，他对自己恶意删除的行为供认不讳，但其动机尚不明确。Sudhish Kasaba Ramesh 使用个人 GoogleCloudProject 账户部署了恶意代码，删掉了 456 台虚拟机，造成 16000 个 WebExTeams 账户被异常关闭。思科因此被客户退款超过 100 万美元，其损失共计 240 万美元（约合人民币 1652 万）。

Sudhish Kasaba Ramesh 将为自己的行为付出代价，面临着 5 年的牢狱生活和 25 万美元的罚款。Sudhish Kasaba Ramesh 也许会因此被驱逐出境，但其目前所在的公司 StitchFix 仍愿为他保留工作岗位。对于此次被前员工恶意删库，思科方面表示交由警方处理，并会进行内部整改，防止类似事件再次发生。

删库跑路事件频发

其实类似的事件已经不是第一次发生了，许多公司都遇到过或是被误删或是被恶意删库的情况。2015 年，携程就曾因员工误删代码导致了官网瘫痪。北京某科技公司的员工还曾因为工资纠纷恶意删除了网站的源代码，最终获刑五年。“删库跑路”的事件频频发生，暴露出的不仅是公司与员工之间信任关系的问题，还反映出了内部审查和制度的不完善。恶意删库的人虽然被抓了，但他造成的直接或间接的损失都是无法估量的。

如何避免此类事件

对企业来说，为了避免程序员“删库跑路”，首先要做好备份，既是事情已经发生也能在最快的时间恢复系统的运行，将损失减到最低。其次是需要选择靠谱的云服务商，做好访问控制，杜绝已离职员工还能远程登陆的情况发生。最重要的还是备份，而且是多地备份。

（来源：安全学习那些事）

➢ 日本移动运营商“都科摩”电子支付系统连续发生多起盗刷

2020 年 9 月 10 日，日本最大的移动运营商“都科摩”的电子支付系统，被曝出接连发生多起盗刷事件，电子支付安全问题再次引发日本社会关注。

在这次电子支付系统盗刷事件中，受害者大多是在手机等移动终端下载了都科摩的支付软件，然后与自己的银行账户进行了绑定。截至目前，已经发现有包括日本邮储银行、永旺银行在内，10 家银行下的账户被盗刷共计 34 次，累计盗刷金额超过 1000 万日元（约合人民币 64 万元）。

目前已知损失最大的单个账户，被多次盗刷共计超过 60 万日元（约合人民币 3.8 万元）。

有关盗刷原因，目前警方分析，有可能是不法分子通过钓鱼软件，窃取了受害者的账户及密码，然后利用电子支付系统的身份验证漏洞实施了盗刷。

昨天，一位受害者在接受媒体采访时透露，本月 2 日，她发现自己存款被盗刷之后，第二天就立即要求冻结账户，然而银行和都科摩双方都表示此事与自己无关、不予理睬。直到后来盗刷事件在日本各地接二连三发生后才着手处理，这也让受害者感到十分难以接受。目前已经有多名受害者表示将向都科摩和银行方面要求赔偿。

盗刷事件发生后，立即引发了业界对于都科摩电子支付系统安全性的广泛质疑，到昨天下午，就已经有 18 家银行陆续宣布不再与都科摩进行新的用户绑定，使都科摩的业务合作及品牌形象受到巨大冲击。就在昨晚，为防止受害范围进一步扩大，都科摩宣布从今天起全面暂停与全部 35 家合作银行的新用户绑定，并表示为提高安全性，今后将加强用户身份验证力度，确保在输入短信密码前无法打开账户进行交易。

实际上，这已经不是日本的电子支付系统第一次出现盗刷事件。去年便利店巨头 7-11 推出的电子支付服务，就曾因安全漏洞问题，导致 800 多名用户被盗刷 3860 万日元（约合人民币 248 万元）。随着日本政府大力推动无现金支付，日本短时间内出现了大约 30 种电子支付服务，其中也暴露出了不少安全措施尚未完善的问题。

专家呼吁，日本电子支付行业整体应该重新审视系统安全现状并制定有效的防范措施。日本金融厅也向各金融机构发出了呼吁，要求高度警惕盗刷行为，并在发现后及时进行调查并报告。（来源：央视财经）

➢ 智利银行遭到勒索软件攻击后：关闭了所有分行

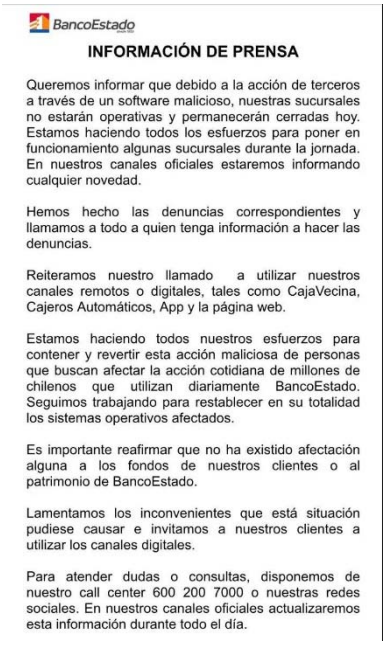
2020 年 9 月 8 日报道，智利国家银行（BancoEstado）的所有分行在 9 月 7 日周一仍处于关闭状态，可能还要停业多日。

智利三大银行之一国家银行在上周末遭到勒索软件攻击后，周一被迫关闭了所有分行。**该银行周一在其推特帐户上发布的一份声明中说：**“我们的分行无法运营，今天仍处于关闭状态。”有关攻击的细节尚未公之于众，但了解调查情况的消息人士告诉 IT 外媒 ZDNet，该银行的内部网络感染上了 REvil（Sodinokibi）勒索软件。目前初步调查后发现，该事件源自一名员工收到并打开了一份恶意 Office 文档。据信，该恶意 Office 文件在这家银行的网络上植入了后门。

调查人员认为，在周五至周六之间的晚上，黑客利用该后门访问了银行的网络，并安装了勒索软件。周末轮班的银行员工在周六无法访问工作文件后发现了这起攻击。国家银行向智利警方报告了这起事件。就在同一天，智利政府发布全国性网络安全警报，提醒防范针对私营部门的勒索软件活动。

据消息人士声称，虽然最初该银行希望在不被人注意的情况下在攻击后恢复过来，但遭到了严重破坏，勒索软件对绝大多数内部服务器和员工工作站进行了加密。

该银行最初在周日披露了攻击事件，但银行官员后来


BancoEstado

INFORMACIÓN DE PRENSA

Queremos informar que debido a la acción de terceros a través de un software malicioso, nuestras sucursales no estarán operativas y permanecerán cerradas hoy. Estamos haciendo todos los esfuerzos para poner en funcionamiento algunas sucursales durante la jornada. En nuestros canales oficiales estaremos informando cualquier novedad.

Hemos hecho las denuncias correspondientes y llamamos a todo a quien tenga información a hacer las denuncias.

Reiteramos nuestro llamado a utilizar nuestros canales remotos o digitales, tales como CajaVecina, Cajeros Automáticos, App y la página web.

Estamos haciendo todos nuestros esfuerzos para contener y revertir esta acción maliciosa de personas que buscan afectar la acción cotidiana de millones de chilenos que utilizan diariamente BancoEstado. Seguimos trabajando para restablecer en su totalidad los sistemas operativos afectados.

Es importante reafirmar que no ha existido afectación alguna a los fondos de nuestros clientes o al patrimonio de BancoEstado.

Lamentamos los inconvenientes que está situación pudiese causar e invitamos a nuestros clientes a utilizar los canales digitales.

Para atender dudas o consultas, disponemos de nuestro call center 600 200 7000 o nuestras redes sociales. En nuestros canales oficiales actualizaremos esta información durante todo el día.

意识到了员工周一无法工作，于是决定在恢复期间让分行处于关闭状态。幸好，该银行似乎做了该做的工作，对内部网络进行了适当的分隔，因而限制了黑客可以加密的内容。据该银行发布的多份声明显示，该银行的网站、银行门户网站、移动应用程序和 ATM 均未受影响，向客户保证他们的资金很安全。

REvil 勒索软件团伙是少数几个运行泄露网站的组织之一，它在该网站上泄露来自从其闯入的网络的文件，以防受害者不愿支付赎金。截至本文发稿时，国家银行的名称不在泄露网站上，这表明该银行不是支付了赎金，就是仍在与黑客进行谈判。

这已是黑客第二次攻击智利银行。2018 年 6 月，朝鲜黑客在企图隐藏银行黑客活动的同时，在智利银行的网络上部署了清除磁盘内容的恶意软件。一年后，这伙黑客还在企图实施 ATM 提现诡计时闯入了 Redbanc，该公司将所有智利银行的 ATM 基础设施互连起来。（来源：ZDNet）

➢ 百名学生中考志愿遭篡改,西昌警方抓获嫌疑人:同窗猜密码泄私愤

2020 年 9 月 4 日，四川西昌某中学的吉某某升学无望，为泄私愤在家中通过自己手机，登录中考志愿填报系统，篡改了上百名同学的中考志愿……记者从西昌市公安局获悉，日前，西昌警方破获一起恶意篡改中考志愿的案件。幸好西昌警方及时介入，并将吉某某抓获归案，当地招办特事特办，延长考生填报志愿时间，组织学校逐一通知考生本人修改志愿，最终圆了这些学生的升学梦。目前，嫌疑人吉某某已被刑拘。

上百名学生志愿被篡改 同窗是幕后黑手

西昌警方介绍，今年 7 月 30 日，西昌市公安局网络安全保卫大队接到报警，西昌市某校学生发现自己的中考志愿被篡改。学校经过初步排查，发现上百名学生志愿被篡改。志愿填报已经停止，该部分学员将无法被录取升入更高一级学府，这些学生面临无法上学的严重问题。

接到报警后，西昌市公安局网安大队紧急抽调专人侦办，迅速查明有人非法破坏计算机信息系统，存在大量考生填报志愿被篡改的情况。该情况社会影响大、危害程度深，按照“净网”工作要求，网安部门立即进行追查，并对志愿填报系统进行漏洞检查，发现系统存在验证机制漏洞等问题。

经过连夜奋战，快速开展工作，警方锁定了涉嫌篡改考生志愿的终端，查证发现为该校毕业学生吉某某使用。经过走访，发现嫌疑人正在山上放牛。山上放牛区域属于野外林地，海拔高度近 3000 米，没有通车公路。专案组从村组出发，迅速步行登山，在山上将吉某某挡获。

为泄私愤篡改同学志愿 猜中同学们的密码

民警迅速查看其随身携带的手机，证实正是大量登录考生账户填报志愿的终端。经查，吉某某升学无望，为泄私愤在家中通过自己手机，复制班主任发在微信群里的 2020 年度初三毕业生名单，登录凉山州中考志愿填报系统，尝试输入密码“12345678”，进入他人账户篡改志愿。

西昌市公安局网安大队按照“一案双查”工作机制，迅速与招办、学校对接，通报了该班主任老师违规发布学生信息的情况。同时针对志愿填报系统无安全保护与验证机制漏洞等问题进行了通报，并针对系统开展了专项检查工作。针对志愿填报系统存在的问题，西昌市公安局网安大队按照《中华人民共和国网络安全法》，对涉案单位依法开展行政处罚工作。

目前这些学生已圆升学梦 嫌疑人被刑拘

民警介绍，根据反馈情况，当地招办特事特办，延长考生填报志愿时间，组织学校逐一通知考生本人修改志愿，确保考生有学可上，最终圆了这些学生的升学梦。目前，吉某某已被刑事拘留。

“其实弱口令问题，网安部门曾多次提醒过。这个案件再一次证明，弱口令会带来严重后果，务必予以重视。”办案民警表示，弱口令非常容易被别人猜到或被破解工具破解，比如仅包含简单数字和字母的口令“12345678”或者姓名全拼、生日等，这种口令轻而易举就会被人破解，从而使用户面临巨大风险。

民警提醒：要强化个人信息保护，不要在微信群等公共平台发布涉及个人信息的内容；加强个人密码保护：一定要修改初密码，密码应包含大、小写字母和特殊字符。（来源：央视新闻）

➢ 江苏宿迁两银行职员盗取客户信息被依法处理

2020 年 9 月 7 日宿迁网警报道，任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。明知出售公民个人信息犯法，但为了赚钱仍然铤而走险。近日，我市成功破获一起非法获取公民个人信息案件，抓获违法嫌疑人 2 人，从违法嫌疑人手机中查获的各类公民个人信息合计 5996 条。

案件回顾

“您好，我是某某银行业务经理张某某，如有任何业务均可向我咨询……”7 月以来，泗洪县某局近 400 余名职工陆续收到同条短信，给职工生活带来诸多不便。接警后，泗洪县

公安局网安大队立即成立专案组开展调查取证，并依法传唤了违法嫌疑人张某某。到案后，张某某主动交代了违法事实。

违法嫌疑人在接受办案民警讯问

经查，“某某通”APP 是众多企事业单位广泛使用的一款手机通讯录软件，该软件数据具有全面和高准确率的特点。自 2020 年 6 月 8 日至 7 月 24 日，张某某在给客户办理银行相关业务时，在客户不知情的情况下，使用客户的手机号码和收到的短信验证码在自己的手机上登录客户“某某通”APP，非法获取客户“某某通”内单位通讯录手机号码 2879 条，用于发送短信推广贷款业务。

无独有偶，民警发现该银行职工李某某利用同样手法，从 2019 年 9 月至 2020 年 8 月，非法获取 6 家企事业单位通讯录手机号码 3117 条，用于发送短信推广贷款业务，给公民信息安全造成极大的威胁。目前，违法嫌疑人张某某、李某某因涉嫌非法获取公民个人信息，被依法处以罚款。

法律链接

《中华人民共和国网络安全法》第四十四条：任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。《中华人民共和国网络安全法》第六十四条第二款：违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

随着互联网技术的不断发展，公民个人信息被他人非法获取和利用的情形时有发生，公民个人信息安全受到很大威胁，不法分子往往利用非法获取的公民个人信息实施其他违法行为。因此，广大网民要注重保护自己的信息；作为合法获取公民个人信息的单位或个人来说，也要进一步强化法律意识，切忌非法向他人提供公民个人信息。（来源：宿迁网警）

➢ 阿根廷移民局遭遇攻击中断服务 4 小时

2020 年 9 月 7 日，阿根廷官方移民管理机构 Dirección Nacional de Migraciones 日前遭受 Netwalker 勒索软件攻击，并直接导致边境入出境事务陷入瘫痪。虽然此前全球各地先后发生多次针对城市及地方政府机构的勒索软件攻击，但此次事件或将成为首例针对联邦政府一级目标发起的已知攻击活动。

根据阿根廷网络犯罪管理机构 Unidad Fiscal Especializada en Ciberdelincuencia 公布的刑事诉讼记录，该国政府于 8 月 27 日上午 7 时左右收到边境检查站的大量技术支持电话，并由此意识到勒索软件攻击的存在。

“当天上午约 7 时，信息系统与技术总局下辖的技术与通信署接到大量求助电话，多处边境检查站要求提供技术支持。”

“技术与通信署旋即意识到问题严重性，并立即对中央数据中心及分布式服务器基础设施进行评估，发现基于微软 Windows 的大量系统文件（主要包括 ADAD SYSVOL 与 SYSTEM CENTER DPM）以及用户在工作与共享文件中保存的微软 Office 文件（Word 与 Excel 等）皆受到一种病毒的影响。”

为了防止勒索软件感染其他设备，移民局与检查站方面很快了关闭所使用的计算机网络。根据阿根廷新闻网站 Infobase 的报道，此次攻击导致边境过境点停摆四个小时，之后服务器重新正常上线。

阿根廷国家移民局（DNM）表示：“国际过境点各检查站运行的综合移民跟踪系统（SICaM）受到的影响尤其严重，并导致阿根廷出入境工作发生延误。”政府内部的消息人士在采访中表示，“他们不会与黑客谈判，也不指望能够取回被锁定的数据。”

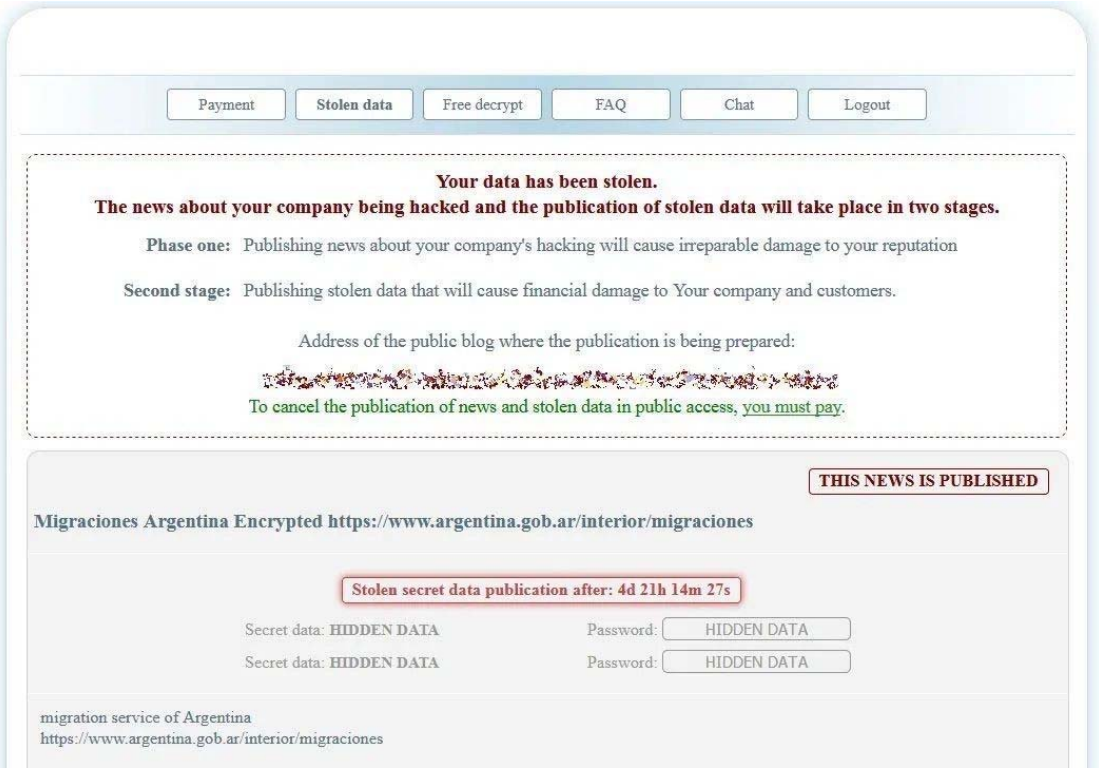
Netwalker 要求阿根廷政府支付 400 万美元赎金

在勒索软件开展攻击的同时，Netwalker 已经在锁定设备上发布了勒索要求。要求中包含指向暗网支付站点的链接，该站点则详细介绍了如何购买解密工具、攻击方开出的赎金金额以及在攻击活动中遭到泄露的未加密文件信息。

在 Netwalker Tor 支付页面中，可以看到勒索软件攻击方最初开出的赎金数额为 200 万

美元。

但在七天之后，赎金总额提升至 400 万美元，约合 355 个比特币。下图所示，为 Dirección Nacional de Migraciones 赎金页面上的内容。



该 Tor 网站还包含一个“被盗数据”页面，展示了在攻击期间从“Migraciones Argentina”处窃取到的数据截屏。由于此次泄露的数据可能较为敏感，因此文章后续将不再发布新的数据泄露截屏。（来源：新浪）