



扫一扫，关注官方微信

联系我们

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

热点 | 亿赛通数据库安全产品正式入驻微软云 Azure

《个人信息安全规范》修订版已发布，这些与你我息息相关
两会声音 | 安全问题如今刻不容缓……



关注企业官方微信

Esafenet Monthly magazines

中国数据安全防护专家



主办：亿赛通

策划：市场部

北京亿赛通科技发展有限责任公司

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com



本刊为亿赛通企业月刊，欢迎交流，禁止转载

CONTENTS 目录

刊首语 PREFACE

2/3 《亿赛通五月刊》一览信息安全行业新动态

行业聚焦 INDUSTRY FOCUS

4-8 国内行业新闻

9-13 国外行业新闻

亿赛通动态 ESAFENET NEWS

14 喜报 | 亿赛通连续多年荣获“北京市诚信创建企业”称号

15 亿赛通数据库安全产品正式入驻微软云 Azure

16-19 网络数据泄露防护你需要知道什么？

20/21 网络数据泄露问题演化升级，亿赛通全新网络数据泄露防护软件解析

22/23 如何做好个人信息泄露防护

亿赛通小贴士 ESAFENET PROMPT

24/25 只要几十元就能离你的爱豆近一点？

26/27 被罚 100 万，原来是因为他……

28/29 谁在倒卖银行内部个人信息？

30/31 两会声音 | 安全问题如今刻不容缓……

32/33 《个人信息安全规范》修订版已发布，这些与你息息相关

典型案例 TYPICAL CASES

34/35 某大型装备集团与亿赛通强强联手，打造中国工程机械行业安全标杆

36/37 长鑫存储技术有限公司

《亿赛通五月刊》 一览信息安全 行业新动态

信息安全保护是一项复杂的工作，除了技术手段、信息安全管理、保密制度等，更需要社会全体一起参与进来，从每一个人的工作习惯、基本安全认知和安全意识等点点滴滴的方面开始重视，信息才能得以更好的保护！两会期间，《个人信息保护法》的加速建立、商家不得收集个人生物敏感信息、疫情期间个人信息的“善后”处理等问题受到社会的广泛关注。信息安全工作与其亡羊补牢，不如提前防范，本期月刊，亿赛通与大家共同剖析信息安全如何采取策略进行防护……



国内

1、全国数据黑产规模已超千亿美元，委员建议提升国家数据安全能力



摘要：全国“两会”期间，在沪全国政协委员、上海众人网络安全技术有限公司董事长谈剑锋在提案中建议，面对数据安全和隐私保护的复杂形势，要从立法、执法、国际合作、产业发展等多个维度综合施策，全面推进国家数据安全综合能力体系建设。

2、两会建议设立疫情个人信息采集退出机制



摘要：两会中建议相关部门统筹联动、做好对疫情相关个人信息的管理以及疫情后的信息处置工作。一是针对新冠肺炎疫情期间采集的个人信息设立退出机制。二是加强对已收集数据的规范性管理，最大限度地降低数据泄露、滥用风险。三是研究制定特殊时期的公民个人信息收集、存储和使用的标准和规范。

3、警方通报女子未点餐被外卖员强送外卖：外卖员已行政拘留

摘要：据南京市公安局江宁分局消息，2020年5月20日，警方注意到有微博用户在新浪微博发帖称在南京江宁遭遇未点餐情况下有外卖骑手上门送餐并准确报出该用户真实姓名事件，引发网友关注。经警方对此事件进行详细调查，现已查明事件始末，特此澄清相关事实，回应网络关切。



4、建行再曝数据泄露事件！ 又一名员工因贩卖客户数据被抓



摘要：近日，江苏省淮安市警方破获了一起由建设银行员工参与，贩卖用户个人信息数据的案件。这是继近期《建设银行支行行长沈静冲因贩卖用户信息数据被捕入狱》后的又一起“建行数据贩卖”案件。

5、江苏警方破获特大“暗网”个人信息贩卖案，5000 余万条信息被泄露



摘要：5月7日，江苏省南通市公安局公布，经过4个多月的缜密侦查，江苏南通、如东两级公安机关破获了一起特大“暗网”侵犯公民个人信息案，抓获犯罪嫌疑人27名，查获被售卖的公民个人信息数据5000多万条。这起案件也被公安部列为2019年以来全国公安机关侦破的10起侵犯公民个人信息违法犯罪典型案例之一。

6、池子银行流水泄露 保障数据安全需多管齐下

摘要：近日，因脱口秀演员“池子”（王越池）指责中信银行在未经授权、未经任何司法机关合法调查程序的情况下，将个人银行账户交易明细提供给与其发生经济纠纷的笑果文化，银行账户信息保密问题引发社会广泛关注。据报道，在黑市上，有人宣称“2000元查一个月流水”。而据银行业内人士表示，理论上只要是银行员工，有内部授权皆可查询。



7、《网络安全等级保护定级指南》等 26 项国家标准获批发布

摘要：根据国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2020年第8号），全国信息安全标准化技术委员会归口的GB/T 20281-2020《信息安全技术 防火墙安全技术要求和测试评价方法》等26项国家标准正式发布。

序号	标准编号	标准名称	代替标准号	实施日期
1.	GB/T 20281-2020	信息安全技术 防火墙安全技术要求和测试评价方法	GB/T 20010-2005, GB/T 20281-2015, GB/T 31505-2015, GB/T 32917-2016	2020-11-01
2.	GB/T 22240-2020	信息安全技术 网络安全等级保护定级指南	GB/T 22240-2008	2020-11-01
3.	GB/T 25066-2020	信息安全技术 信息安全产品类别与代码	GB/T 25066-2010	2020-11-01
4.	GB/T 25067-2020	信息安全技术 安全技术 信息安全管理体系审核和认证机构要求	GB/T 25067-2016	2020-11-01
5.	GB/T 28454-2020	信息安全技术 安全技术 入侵检测和防御系统 (IDPS) 的选择、部署和操作	GB/T 28454-2012	2020-11-01
6.	GB/T 30284-2020	信息安全技术 移动通信智能终端操作系统安全技术要求	GB/T 30284-2013	2020-11-01
7.	GB/T 34953.4-2020	信息安全技术 安全技术 匿名实体鉴别 第4部分：基于密钥的机制		2020-11-01
8.	GB/T 38625-2020	信息安全技术 密码模块安全检测要求		2020-11-01
9.	GB/T 38626-2020	信息安全技术 智能网联设备口令保护指南		2020-11-01
10.	GB/T 38628-2020	信息安全技术 汽车电子系统网络安全指南		2020-11-01
11.	GB/T 38629-2020	信息安全技术 签名验证服务器技术规范		2020-11-01
12.	GB/T 38631-2020	信息安全技术 安全技术 GB/T 22080 具体行业应用 要求		2020-11-01
13.	GB/T 38632-2020	信息安全技术 智能音视频采集设备应用安全要求		2020-11-01
14.	GB/T 38635.1-2020	信息安全技术 SM9 标识密码算法 第1部分：总则		2020-11-01
15.	GB/T 38635.2-2020	信息安全技术 SM9 标识密码算法 第2部分：算法		2020-11-01
16.	GB/T 38636-2020	信息安全技术 传输层密码协议 (TLCP)		2020-11-01
17.	GB/T 38638-2020	信息安全技术 可信计算 可信计算体系结构		2020-11-01
18.	GB/T 38644-2020	信息安全技术 可信计算 可信连接测试方法		2020-11-01
19.	GB/T 38645-2020	信息安全技术 网络安全事件应急演练指南		2020-11-01
20.	GB/T 38646-2020	信息安全技术 移动签名服务器技术要求		2020-11-01
21.	GB/T 38647.1-2020	信息安全技术 安全技术 匿名数字签名 第1部分：总则		2020-11-01
22.	GB/T 38647.2-2020	信息安全技术 安全技术 匿名数字签名 第2部分：采用群签名机制的机制		2020-11-01
23.	GB/T 38648-2020	信息安全技术 蓝牙安全指南		2020-11-01
24.	GB/Z 38649-2020	信息安全技术 智慧城市建设信息安全保障指南		2020-11-01
25.	GB/T 38671-2020	信息安全技术 远程人脸识别系统技术要求		2020-11-01
26.	GB/T 38674-2020	信息安全技术 应用软件安全编程指南		2020-11-01

8、台湾两大炼油厂遭受勒索软件攻击，加油站混乱



摘要：根据 taiwannews 报道，台湾的两个最大的炼油厂（CPC 和 FPCC）两天内相继遭遇网络攻击者的袭击，波及整个供应链，甚至影响到在加油站加油的客户。CPC 首先受到攻击，而 FPCC 在第二天也遭受攻击。5月4日，对 CPC 的攻击使其 IT 和计算机系统关闭，加油站无法访问用于管理收入记录的数字平台。

9、四名辅警出售公民车辆信息被判刑：层层倒卖一条售价 80 元



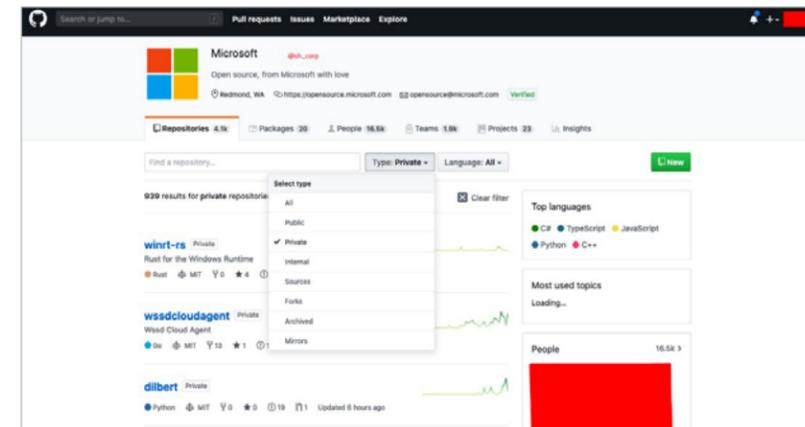
摘要: 浙江省乐清市白石交警中队辅警葛某某、赵某某利用职务之便，查询下载公民个人车辆档案信息（包括车辆牌照、车主信息、抵押情况等）330 余条，并出售给下线潘某某，每条价格为 30 元。不仅如此，葛某某还让同事毛某某、徐某帮忙下载个人车辆档案信息，并以每条 20 元的价格购买。其中，毛某某下载个人车辆档案信息 140 余条，徐某下载 70 余条。

10、B 站知名 up 主遭勒索



摘要: B 站 up 主——机智的党妹（粉丝 557 万）发布了一条视频《我被勒索了！》，随着粉丝阅读、关注度越高，UP 主的视频质量也在提升中。原本通过普通的家庭电脑和硬盘就能存储、剪辑的视频素材，可能增长至几百 G，从而对于视频存储设备提出了更高的要求。在这样的背景下，“党妹”花费十几万，在公司内部网络搭建了一个 NAS 系统。然后，投入使用第一天，被黑了。目前，通过日志仅能查到 IP 位于北京的一家图书馆（但 IP 也很有可能是伪造的）。而此次攻击疑似利用 Buran 勒索病毒。

1、微软 GitHub 账号疑似被黑，黑客声称窃取 500GB 数据



摘要: 根据 BleepingComputer 透露的消息，一名黑客声称自己成功入侵了微软的隐私 GitHub 库，并从中窃取了超过 500GB 的数据。微软公司尚未就该漏洞事件公开发表评论，这似乎并没有影响到该公司任何主要软件产品。在此攻击事件发生之后，以为自称名叫“Shiny Hunters”的黑客与 BleepingComputer 联系，并告知称他已经成功入侵了微软的 GitHub 账号，而且成功获取到了其私有 GitHub 库的完整访问权。

2、秘书公开展示特朗普捐款支票 不料泄露了总统私人账户信息



摘要: 据《纽约时报》报道，美国当地时间 5 月 22 日，白宫新闻秘书凯莉·麦克纳尼在新闻发布会上宣布，特朗普将把 10 万美元的季度工资捐给美国卫生与公众服务部，以帮助应对新冠肺炎疫情。麦克纳尼还在发布会现场向媒体展示了捐款支票。不料支票上面，特朗普的私人银行账户和路由号码等个人信息清晰可见。

3、以暴制暴？黑客入侵并加密诈骗分子电脑



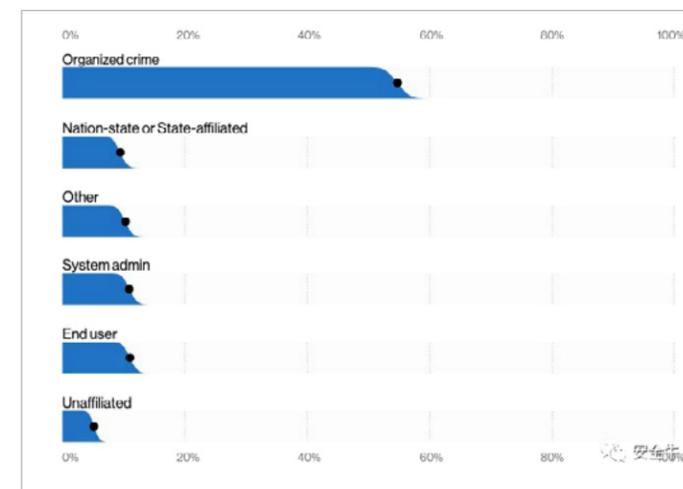
摘要：最近，有黑客组织发起了专门针对这些诈骗组织的攻击。这个名为 CyberWare 的黑客组织以一款新型的勒索软件 MilkmanVictory 来入侵那些诈骗团伙的计算机。CyberWare 说他们目前在攻击那些借款诈骗的团伙，即是那种向受害人表示可以提供贷款，但是需要受害人先打款过去，最终导致受害人损失一大笔钱的诈骗。CyberWare 会向这些诈骗团伙发送含有勒索软件伪装成 PDF 文件的邮件，但是与一般中招后会显示付款方式来解密不一样，这个软件并不会要求他们付款，而只会显示一句话表示他们的计算机文件已经完蛋了。

4、英国易捷航空遭黑客入侵，约 900 万客户个人信息被窃取



摘要：英国廉价航空公司易捷航空 EasyJet 的一份声明称，在一次重大数据泄露事件中，约 900 万客户个人信息被窃取，其中包括 2200 名客户的信用卡详细信息也被获取，但护照记录暂未发现泄露。易捷航空没有透露安全事件是何时发生的，也没有说明黑客是如何进入其系统的。

5、Verizon 年度数据泄露报告：金钱依然是第一动力



摘要：Verizon 近日发布的年度数据泄露调查报告 (DBIR) 显示，金钱依然是网络攻击的第一动力。研究人员分析了 32,002 起安全事件，这些事件导致了信息资产的泄露。在这些事件中，有 3,950 起是数据泄露事件，即导致向未授权方确认数据泄露的事件。亮点和发现如下：70%的数据泄露行为是由外部行为者实施的（医疗保健行业除外，该行业 51%是外部行为，48%是内部行为）86%的泄露是出于经济动机；有组织犯罪集团的违规行为占 55%；72%的数据泄露涉及大型企业。

6、欧洲多地超级计算机感染挖矿木马，疑为同一攻击者

摘要：欧洲突然曝出多达十数台超级计算机感染恶意挖矿软件，沦为挖矿肉鸡。英国爱丁堡大学首先公布了 ARCHER 超级计算机遭到攻击的报告，表示关闭 ARCHER 的系统进行调查，并且为了防止再次被攻击，重置了 SSH（安全外壳协议）密码。同一天德国超级计算机管理组织 bwHPC 宣布因为类似的安全问题，旗下 5 台超级计算机 / 高性能计算集群 bwUniCluster 2.0、ForHLR II、bwForCluster JUSTUS、bwForCluster BinAC、Hawk 现起关闭。

7、澳大利亚一物流货运巨头被黑客勒索，不交赎金就泄露客户数据



摘要：澳大利亚物流和货运巨头 Toll Group 在短短三个月内遭受了两次黑客袭击。为避免进一步的风险，成为勒索软件的受害者，Toll Group 关闭了其 IT 系统和客户接口。据悉，黑客渗透了一个包含有关 Toll 现有和前雇员和客户信息的服务器，但 Toll 并未屈服于对方要求以赎金换取再次被入侵数据的要求。

8、印度最大在线教育平台 Unacademy 发生大规模数据泄露



摘要：近日，印度最大的在线教育平台 Unacademy 承认发生数据泄露事件，暴露了大约 1100 万用户的个人详细信息。网络安全情报公司 Cyble 表示已收购了一个包含近 2200 万个 Unacademy 用户账户的数据库（Unacademy 在声明中指出自己只有 1100 万用户），该数据库在暗网上的售价为 2,000 美元。泄漏的数据包括用户 ID、名称和用户名、加密密码、电子邮件地址、加入日期和上次登录时间。

9、任天堂遭史上最严重黑客攻击：完整源代码、设计文档及技术演示泄露

```

-Source code for boot0/1/2
-Block diagram/datasheets for every system component & Verilog for AES/SHA
-Documents from BroadOn describing feature planning and implementation + APIs + docs for internal software
-Full IOS SDK
-Source code for IOS (IOS is the Wii Operating System)
-Planning docs for implementation of the system from 2004-2006
-some wii sdk library source code (DVD, EXI)
-source code and info on manufacturing and publishing systems
-some misc. nintendo stuff (internal WPAD SDK from 2005, Wii Overview from RVL_SDK 1.0)
-"sdboot", a special manufacturing version of boot2 which loads data from the SD card; is very buggy and likely exploitable for boot2 code execution on all Wiis (it is retail signed)
-gamecube and ique stuff as well (internal gamecube docs including physical disc layout, massive 2GB+ iQue dump including full CVS for that as well)
    
```

摘要：过去数周时间里，有位匿名用户在美国论坛 4chan 中，陆陆续续上传了大量任天堂内部档案。此外，Youtube 博主 Sebastian 也整理了类似 N64 游戏的 Demo。Resetera 网站用户 Atheerios 密切关注了此次事件，他认为，所有的数据、文件都直接从一家和任天堂合作的公司 (BroadOn) 内部窃取。黑客通过攻击 BroadOn 服务器，获得了 Wii 主机的所有源代码、数据表、设计框图以及每一个配件的 Verilog 文件 (Verilog 是一种硬件描述语言)。

10、Google Chrome 惊爆重大安全漏洞！10 亿国人浏览器将陷入巨大风险



摘要：根据大数据统计，国内有 85% 的浏览器是基于 Google 公司的 Chromium 开源项目进行二次开发而来，包括著名的某安全浏览器，某双核浏览器等等，但在近日 Google 发布 Chrome 网络浏览器安全更新，包含针对重大安全漏洞的修补程式。但因不希望邪恶黑客利用漏洞发动攻击，因此除了表示漏洞涉及 [语音辨识模组 『使用释放后记忆体』 (Use-After-Free, UAF) 漏洞]，就没有透露更多细节。

喜报 | 亿赛通连续多年荣获“北京市诚信创建企业”称号



喜报 以诚为本，不忘初心

近日，经宣贯动员、企业自愿申报、信用信息采集、第三方机构征信、行业协会初审、专家组综合评审，在全市范围内共评选出“北京市诚信创建企业”，北京亿赛通科技发展有限公司再次从全市数百万企业中脱颖而出，获此殊荣。

如今，社会关注企业专业技术的同时，更在乎的是企业是否存在信誉、服务漏洞等问题。“德盛者其群必盛，德衰者其群必衰”，对一个品牌、一家企业来讲，诚信是灵魂、是生命、是企业生存和发展的永恒的动力。企业即使拥有一流的产品但公司信誉过低，导致客户的基本权益得不到保障，也不是一家成功的企业。

北京市企业诚信创建活动由北京市经济和信息化局、首都精神文明办、市工商局、市地税局等共同发起，是北京市诚信文化建设的品牌项目，也是落实推进诚信

建设，强化社会责任意识、规则意识、奉献意识的具体举措。诚信创建结果将纳入市工商局的《北京市企业信用信息网》进行公示，并发布到北京市公共信用信息服务平台供社会查询。

作为国内数据安全企业迎风招展的一面旗帜，专注技术创新，诚信经营，服务客户，始终是亿赛通这个屹立中关村十七年的数据安全企业的创立初衷与运营使命。未来，亿赛通将继续践行诚信经营理念，积极履行社会责任，把产品和服务做到让用户放心、满意，把品牌做到有口皆碑，为中国品牌和诚信社会的建树，做出竭诚贡献。

关于亿赛通

亿赛通以数据资产防泄密为核心，以网络安全为基本框架，以协议识别解析为技术支撑，对数据进行智能识别、智能分类、智能加密，保障企业核心数据资产安全无泄露，打造数据安全领域真正意义上的综合解决方案！

亿赛通数据库安全产品正式入驻微软云 Azure

近日，亿赛通数据库安全系统正式入驻微软云平台，向全体用户提供更加便捷、更加安全的数据库安全解决方案。

独立数据安全服务商，保护数据库安全

眼下，各行业数据库安全环境的复杂程度今非昔比，网络安全威胁不断升级，如信息泄露、未知威胁、网络入侵等层出不穷。可见，用户对安全体系的效能与可信、合法合规，有了更深刻的需求。面对日新月异的黑客技术迭代，如何有效对抗新威胁、快速适应安全新环境，提升数据库安全性、让数据信息的安全得到充分保障，成为用户抢占制高点的关键。

亿赛通数据库安全系统不仅能够为企业节约成本、增强数据库管理的灵活性，还可享受智能快速的安全保障。此次以专业团队为支撑的数据库安全服务，以客户使用感受、操作流程为第一位，成功入驻微软云，在中国数据安全领域又一次独领风骚，占领数据库安全市场。

下面小编将为您打开“数据库安全系统”的微软云操作流程，简单购买、简单应用、让一切变得简单！

提示

购买后需要联系我司工作人员才能获得产品授权哦，如果有任何问题也可以咨询服务人员：400-898-1617

未来亿赛通产品将与微软云深度合作，多数产品即将上云，使得用户购买使用更加便捷；而亿赛通数据库安全产品对于企业级用户而言，将享有更加开放、实用的数据库安全服务。亿赛通十七年来专注于数据安全，提供专业的数据安全落地方案，对数据的全生命周期“存、管、用、销”的全路径实现安全防护。符合网络安全法、数据安全法、等保 2.0 等法律法规要求，可有效减少核心数据资产被侵犯的可能性，保障正常的业务连续性。

第一步

打开“微软云”平台页面，即可查看亿赛通数据库安全系统（DAS）产品介绍。



第二步

选择计划 + 定价，即可查看产品价格、配置等情况，用户可根据自己需求下单购买。



网络数据泄露防护你需要知道什么？

产品管理与解决方案部：张兴堂 / 文



1. 方案背景

互联网给人们的工作带来了极大的便利，但是也极易发生数据泄漏的途径。在全球范围内，因企事业单位在互联网管理上的工作疏忽，导致数据泄漏事件越来越多，而给企业造成的经济损失也越来越巨大。因此越来越多的企业开始意识到数据防泄漏的重要性，有的企业甚至在 10 多年前就已经部署和使用了数据防泄漏的产品。对于任何一个企业来说，数据安全防护，加强网络数据防泄漏管理已经成为刻不容缓的事情。

1.1 政策法规指引

用户个人信息的潜在价值刺激着人们不断收集和使用数据的欲望，巨大的经济利益催生地下产业链非法牟利，严重威胁用户个人信息安全。因此，需要制定个人信息保护的标准，遏制数据时代个人信息安全的系统性风险。个人信息保护标准首先应引导重点行业开展个人信息安全相关国际标准和国内标准的实施认证，其次要规范个人信息处理的全流程活动，规定个人敏感信息在收集和利用之前须获得个人信息主体明确授权。随着我国个人信息滥用问题日趋严重，社会对个人信息保护立法的需求越来越迫切。

在 2018 年 9 月公布的“十三届全国人大常委会立法规划”中，《个人信息保护法》与其他 68 部法律被列为“条件比较成熟、任期内拟提请审议的法律草案”。《个人信息保护法》从源头保护做起，从信息获得的源头建立制度，并采取综合手段保护，以行政法规、民法规则和刑法规则相结合的综合治理的方式来建立信息保护制度。

因此，2020 年 2 月，中国人民银行发布了《个人金融信息保护技术规范》；

2020 年 3 月，全国信息安全标准化委员会（以下称“信安标委”）正式发布了《信息安全技术个人信息安全规范》；

两大标准的发布就此奠定了我国个人信息保护的技术指引方针和实施策略。

2. 企业风险分析

随着企业的高速发展和信息化工作的推进，越来越多的公司涉密文档和个人信息以电子化的形式流转，一方面极大的提高了工作效率，另一方面也令泄密风险俱增，这些文档一旦失控，损失将会难以估计。

由于目前企事业单位的所有个人信息数据、合同类文档、财务类文档、知识产权类文档、技术研发、设计、归档管理的资料均无形成适合整个集团的整体防护手段，在日常工作中如缺乏妥善管理，没有对文档的传输使用进行控制，文档 / 敏感信息在互联网的外发风险时刻存在，并将来的任何时刻都可能造成重大的数据泄漏事故，给企事业单位造成极大的财务风险、行政管理风险。

2.1 数据风险

敏感数据分布在企事业单位的各个角落；

敏感数据泄漏可能发生在企事业单位中的任何人员上；

敏感数据的泄漏可能发生在任何时间；

敏感数据的传输风险可能发生在任何一种网络应用中。

2.2 人员风险

信息泄密事件的发生大多数和人密切相关，泄密的途径和方式也多种多样，可概括为如下三方面：

2.2.1 主动泄密和被动泄密隐患

不管是主动泄密还是被动泄密已经成为当前企业信息安全的首要问题，据报告数据显示，目前泄密事件 78.9% 的损失都是由内部人员泄密导致。可导致数据泄漏的常用网络应用包括：邮件、论坛、微博、网盘、FTP 服务、SMB 服务等；

2.3 管理风险

缺乏在网络端的数据防泄漏手段不能有效预防核心数据主动、被动网络泄密风险；

数据通过网络外发后没有记录，出现问题无法溯源；

数据通过网络外发后没有及时发现，不能及时响应控制；

缺乏有效的统计分析，不清楚企事业单位存。

3. 建设方案

3.1 建设目标

本方案是在企事业单位的网络出口端，建立最后一道关卡，通过网络数据防泄漏系统（NDLP）为企事业单位的数据外发把好最外层的安全防护门。系统以软硬件一体机的形式部署在企事业单位的互联网出口，采用网络数据全流量解析、敏感数据策略识别审计、高危数据识别后传输阻断模式，最大化的保证客户数据的安全管理控制，把数据外发风险降低到最小化。

3.2 建设方案

网络 DLP 产品的核心价值，包括敏感数据日常网络监测、事中违规阻断控制、事后追根溯源，全方位的技术服务，以保证客户数据的安全性。



日常网络监测

网络 DLP 产品部署完成后，会对经过系统的网络流量进行 7 层协议分析，分析粒度达到内容级，在分析过程中实现对网络协议数据的内容敏感性匹配，满足内容级审计需求。审计数据长期保存，支持对数据的浏览，查看，统计分析，趋势分析，报表生成等。

违规阻断

网络 DLP 可实现敏感信息阻断功能，在网络协议中一旦发现客户认为严重的数据泄露事件，系统会自动按照策略处置设置进行敏感数据的传输阻断操作，达到防患于未然。

追根溯源

产品将网络信息进行全量分析和存储，即使在策略配置不及时的情况下也会把历史网络传输数据保存下来，客户可以随时对以往的数据进行分析查看，找出遗漏的数据传输泄露的事件，达到疏而不漏的效果。

3.3 方案优势

全面的网络信息获取

产品提供了全流量网络协议数据分析能力，有效的解决了在策略下发不及时、不准确情况下的网络数据审计数据丢失问题。

产品支持了 IPv4 和 IPv6 双栈协议，保证互联网应用协议的全面支持。

产品支持了日常用到的大部分数据访问和传输协议，并且支持对互联网应用协议的扩容定制化，保证协议数据获取的全面性和及时性。

准确的内容分析、识别能力

产品采用多种数据处理和运算技术，保证了数据获取、分析、识别、统计的准确性，为客户提供最佳的数据识别服务：

采用多通道处理，流量智能平衡技术，实时处理网络信息，实现准确的协议信息还原；

多线程、多模式并发策略识别，准确识别出网络流量中的敏感信息；

多维度的信息统计方案，将信息的多个角度呈现在客户面前，实现总体信息准确掌控；

采用大数据的预处理运算机制，从多个角度对信息进行分析、比对、匹配，实现了一张报表看清所有信息的能力；

快速的数据处理分析能力

为了保证服务响应的时效性，系统在多个角度进行成品性能提升：

协议分析：采用多通道处理，流量智能平衡技术，快速实时处理数据库访问流量；

策略匹配：协议分析与策略匹配在内存中进行，采用多模匹配算法，并行匹配输出；

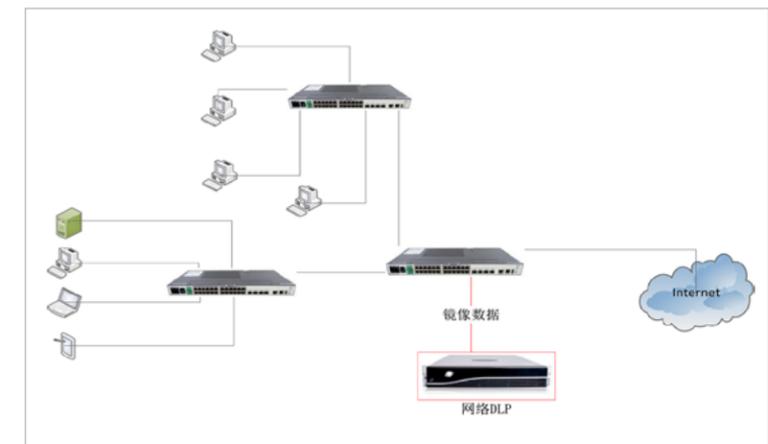
数据入库：多线程、多链接并发入库，大数据处理能力，实现数据秒级数万条写入；

检索分析：采用大数据架构及分片快速索引技术，在亿级数据量下可实现秒级响应；

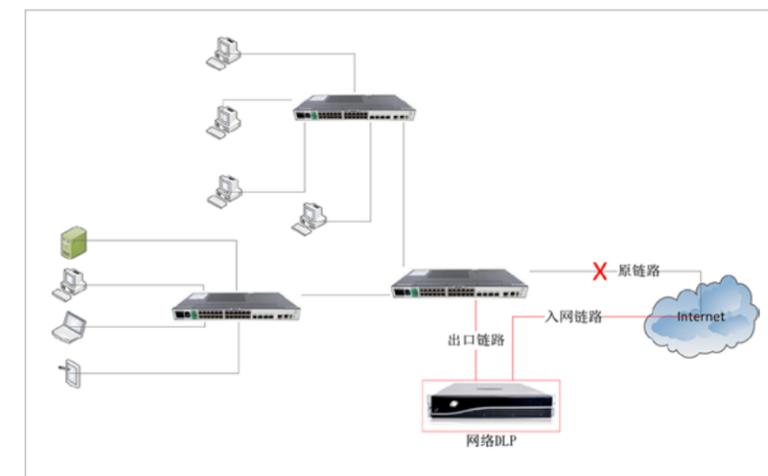
支持多种部署形式

产品在单机部署方面支持旁路部署和串路部署两种方式。

单机旁路部署：型号丰富，满足旁路模式下不同流量和网络接口数据处理性能需求。



单机串路部署：满足 HTTPS 加密协议应用数据识别分析的客户需要，同时支持了在不同流量和网络接口下的型号细分选择。



网络数据泄露问题演化升级， 亿赛通全新网络数据泄露防护软件解析

售前技术部：崔超侠 / 文



网络层数据治理必要性

随着信息化的飞速发展，人们的沟通越来越多的依赖网络。信息化技术给信息传播带来便利的同时，也给信息泄密制造了“温床”。

据统计，80%的信息泄密来源于企业内部，20%的信息泄密来源于网络攻击。因此，传统的防火墙、入侵检测、网络防病毒已经不能完全解决数据泄密事件，企业急需一套应用层网络安全防护方案。

客户主要需求场景如下：

- 1、企业外发流量有统一出口，但是没有专门审计外发数据内容的工具；
- 2、公司应用软件比较多，终端外发数据场景复杂，管理难度大；
- 3、无法对外发文档的内容做识别、管控、审计。

传统网络层数据治理尚存在弊端

传统的网络层数据安全防护主要根据策略匹配外发流量内容，发现敏感数据后做响应，但是传统网络层数据防护弊端比较多：

单台机器无法满足客户需求。针对应用系统比较多的客户，不仅有非加密协议应用（如 HTTPGET，HTTPPOST 等），还可能有加密协议应用（如新浪，搜狐，百度网盘等）。此时旁路部署仅能审计到非加密流量，如要审计加密流量，需要另外再加一台设备串联部署。

传统的网络层数据防护软件策略下发不准确。传统网络层数据监控软件需要提前下发策略，系统会根据策略内容匹配外发数据，发现敏感数据后再做出响应。策略的制定只靠调研是不准确的，如果策略下发太宽泛，容易造成误报，如果策略下发太窄，很容易漏掉一些数据，因此项目落地比较困难。

传统的网络层数据治理工具只支持 IPV4 网络，但是部分军工行业已经使用了 IPV6 网段，因此无法满足实际市场需求。

亿赛通最新网络层数据治理方案

亿赛通最新的网络层数据防护软件充分了解市场需求，根据客户实际应用场景不断优化产品，为客户带来全新的使用体验，产品已于 4 月正式发布。

1. 对于既有旁路部署需求又有串路部署需求的企业，亿赛通一台设备搞定。
2. 先海量审计网络出口数据，后精准下发策略，让企业真实的看到外发数据，合理的管理外发数据。

3. 同时支持 IPV4 和 IPV6 两种协议，为提前使用 IPV6 网络的企业保驾护航。

4. 新网络层数据防护软件不仅保存了原有功能，还丰富了以往的策略库、针对策略配置做了集中化管理、在项目实施部署时更简单。

5. 后台提供丰富的数据查询、统计、分析及报表功能。

6. 系统界面做了全新优化，后台更友好易用，系统具有良好的可扩展性等。

如何做好个人信息泄露防护

售前技术部：夏友军 / 文



随着互联网的运用越发广泛，我们生活的方方面面基本都被互联了起来。但享受了互联生活所带来的便利的同时，生活中的每一个细节却被互联网记录了下来。

同时随着信息技术的不断进步，人们也越来越关注个人信息的安全性。我们也时常在电视或者其他媒体上看到因为个人信息泄露而给个人带来各种各样的麻烦，在信息技术高度发达的今天，一个非常不经意的行为就可能把自己的信息泄露了。所以在大数据面前，我们基本上是“赤裸的”。

那么对个人来说我们应该如何防范个人信息的泄露呢？建议做到以下几点：

1、网站注册时谨慎填写真实个人信息。

某些网站由于安全措施不强，容易被黑客所攻击，从而导致网站注册用户的信息泄露，对个人来说是很大的风险。

2、谨慎上传身份证照片，上传身份证时在照片上加上表示用途的文字。在密码找回、支付工具认证、网上申请信用卡的时候需要我们上传身份证照片，一定要谨慎。上传照片时一定要加上表示该照片用途的文字水印。

3、不在公共场所随意连接未知 wifi，尤其是未加密的 wifi 热点。连接未知的 WiFi 可能会在我们使用该 WiFi 的过程中个人信息就不知不觉地被黑客所窃取，尤其是未

加密的 WiFi，传输数据也是未加密的，因此极易造成信息泄露。

4、谨慎对手机中的各类 app 授权位置和通讯录权限。手机在使用过程中有可能会安装很多应用软件，一些未知的软件在安装的时候不要轻易授权通讯录和位置等权限，防止被某些软件恶意收集相关的个人信息。同时要养成良好的上网习惯：不安装来历不明的软件，不打开危险链接，不浏览非法网站。

对企业来说是否也面临个人信息泄露的问题呢？

目前很多互联网服务公司、电信运营商、银行、中介机构、房地产开发商、保险公司、快递公司、外卖机构、淘宝卖家等组织机构或企业、个人都在长期的经营中，逐渐形成并积累各自的用户信息数据库。

其中涉及会员和客户的信息，如 姓名、性别、年龄、生日、住址、电话、银行账号等大量个人基本信息。有的因管理不善而导致“被动泄密”，有的则是“主动泄密”，有些甚至违反职业道德和保密义务，将这些消费者信息数据窃取后出售牟利。

针对这些企业面临的个人信息泄露的风险，亿赛通也可以提供企业级的网络数据防泄露解决方案，尤其适用于目前非常广泛的互联网应用场景：

1、识别日常网络应用中的敏感内容信息，识别能力包括：

支持预置正则表达式（手机号、身份证号、银行账号等）识别，同时系统支持客户自定义正则表达式识别。帮助用户快速定位敏感个人信息的内容，精准分析做到一旦发送敏感内容可及时发现告警。

系统支持关键词识别，包含关键词的内容识别、关键词指定网络应用识别、多个关键词的组合识别。系统提供关键

词行业字典库，内置的行业字典库包含有金融、地产、医药、财务、证券、政府等多个行业的敏感关键词库，使得客户在系统使用中不再因为敏感信息的设置困难而受阻。

2、识别日常网络应用场景的分析

可以发现和关联到日常用户使用的各种软件应用，运维审计中可以非常直观的查看和识别。

常见的应用包括如：邮箱（QQ，网易 126，网易 163，新浪，搜狐）、论坛（猫扑，天涯，凯迪论坛，水木社区，泡泡俱乐部，百度贴吧，豆瓣，知乎）、微博（新浪微博）、网盘（微云，百度网盘）等。

可以在发现敏感违规泄密行为的时候准确定位和分析。在审计中可以有效追溯和稽查。

基于以上几点通过在企业网络边界处部署亿赛通网络级的 DLP 产品可以有效的管控企业内部通过互联网发送出去的各类敏感个人信息的数据。帮助实现企业内部的个人信息防泄露的安全管理，达到内部管控的要求，同时实现可审计可追溯到目标。

只要几十元就能离你的爱豆近一点？

由于《网络信息内容生态治理规定》的实施，微博近两个月进行了专项治理行动。目前已处罚售卖明星隐私账号 441 个。其中一个违规账号晒出的明星名单囊括了 TFboys、火箭少女、蔡徐坤等当红明星。

关注

#蔚蓝计划# #打击黑产 刻不容缓#为期两个月的内容生态治理专项行动已告一段落，此次专项行动主要是依据《网络信息内容生态治理规定》，针对微博重点位置内容生态、娱乐信息内容生态，黑产信息内容生态展开的一场打击行动。

截止目前共治理重点位置的内容（包括热门微博主贴和色情低俗相关信息）约 26.5 万条，处罚相关账号 2.3 万个，其中高粉丝量账号 225 个。

在打击明星黑粉方面，共处罚黑粉用户 164 个，处罚售卖明星隐私账号 441 个。



明星信息售价低廉

调查后发现一趟国内航班信息的售价是 5 元，节目录制地址加上明星入驻酒店信息的售价是 10 元。此外，明星的身份证、手机号等信息是统一价格，不同卖家的单个号码售价在 15 至 35 元不等。

另外，比较活跃的明星的身份证号可以打包出售，售价在 400 到 600 元之间。行业内招收代理，在收取代理费 188 元后，上家分享自己现有的所有资源，之后明星的身份证、手机号、行程等所有信息的单价都是 5 元，代理者购买后可高价出售，赚取差价。

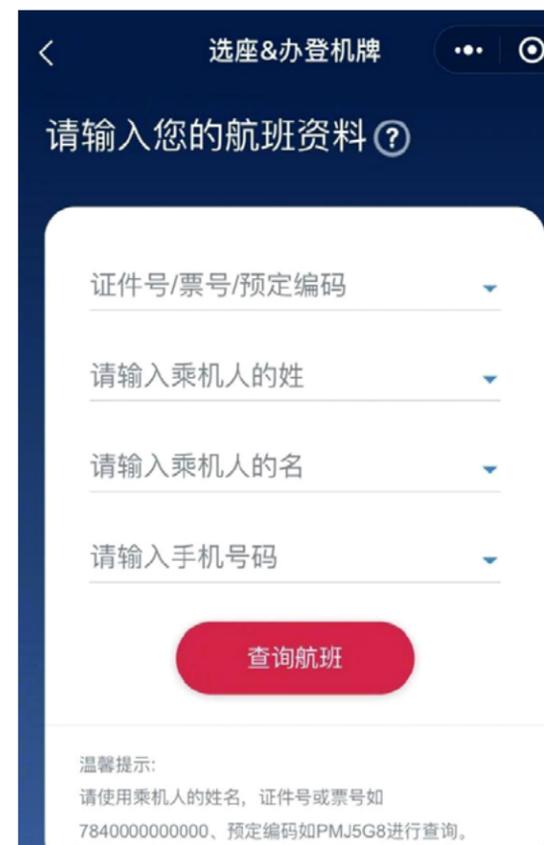
航班信息可漏洞查询

至于明星信息泄露的源头，有些是从机场、酒店、路演现场的一些别有用心的人员中泄露的，有些是不法分子利用技术手段盗取的。

卖家朋友圈每天更新近 20 多条，全部都是各个明星的航班行程、酒店地址等信息。在了解通告行程的前提下，卖家会利用已掌握的明星身份证号来查询航班。比如，打开某航空公司的小程序后，一般会有“选座值机”的界面，通过输入明星的姓名、身份证号和手机号等就可以看到航班的具体信息。有些航空公司（小程序）在输入信息后即可查看。很多卖家正是通过这样的漏洞，查询到了明星的航班信息。

多位明星公开发声痛斥贩卖信息黑产业链

近年来，明星因手机号、身份证号等隐私泄露，遭遇了很多骚扰。仅去年就有多个明星因不堪其扰，在社交平台公开发声。



2019 年 10 月，SNH48 成员陆婷的粉丝在借款平台借款时被拷走手机通讯录，内有该粉丝此前通过不明渠道购买的陆婷及另一位偶像手机号。

2019 年 8 月，王一博在微博公布的通话记录显示，已有 194 个未接来电，平均每隔 3 分钟就有陌生号码来电。

2019 年 8 月，张艺兴身份证号、家庭住址、QQ 等个人信息被曝光，更有甚者盗用张艺兴的个人信息报名登记了器官捐赠。

触犯法律的界限将受严惩

《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》第三条明确规定：向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的，应当认定为刑法第二百五十三条之一规定的“提供公民个人信息”。

根据《刑法》，违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

在整个明星信息买卖链条中，窃取者有之，传播者有之，购买者有之，旁观者有之，暗潮涌动，冲击的不仅仅是明星这一特殊群体的权益，明星的信息几十元就能买到，那么普通人呢？这黑产背后，或许还有很多东西值得我们去思考。作为数据安全服务厂商，中国数据安全防护专家——亿赛通有义务也有责任帮助大家做好数据安全防护工作，最后提醒大家，追星需要热情，但更需要理性，不购买明星信息，与明星保持适当距离，这才是追星的正确打开方式！

文章资讯来源于互联网

被罚 100 万，原来是因为他……



警方曾连续接到多名群众报案，称银行卡被人盗刷。明明银行卡既没有丢失，也没有离开过身边，甚至并未收到短信提醒，账户中的资金怎么能被用于网络购物或转账呢？

这到底是怎么回事呢？

经过警方的调查和研判，最终锁定犯罪嫌疑人浦某并将其抓获。浦某供职于上海某科技有限公司，该公司在为云南某公司开展短信网关项目的开发、建设、维护时，未严格落实网络安全保护工作的要求。在对短信网关系统升级时，未及时发现程序漏洞，以至于部分客户短信在传输过程中以明文形式呈现。浦某负责该公司系统维护，他注意到了这一点，利用工作便利和程序漏洞，获取公民个人信息实施犯罪。

别人的钱真的能免密使用吗？

网警调查发现，浦某的笔记本电脑中存有 4.5 万余条公民个人隐私信息，包括身份证号、银行卡号、手机号、银行验证码等。他利用其非法获取的公民个人隐私信息，将受害人的银行卡绑定在自己的网购平台账户上，同时开通 1000 元以下免密支付，在盗刷的时候不被受害人察觉。在 8 个月的时间里，浦某利用购物、套现等方式先后 60 余次盗刷 50 余名受害者的银行卡 6 万余元。

隐私泄露风险从哪来？

第一：技术安全风险因素

- ① 重视不够，投入不足。
- ② 安全体系不完善，整体安全还十分脆弱。
- ③ 关键领域缺乏自主产品，高端产品严重依赖国外，无形埋下了安全隐患。

第二：人为恶意攻击

相对物理实体和硬件系统而言，精心设计的人为攻击威胁更大。人的因素复杂，思想活跃，不能用静止的方法和法律法规加以防护，这是信息安全所面临的巨大威胁。

第三：信息安全管理薄弱

信息泄露、破坏信息的完整性、拒绝服务、非法使用（非授权访问）、窃听、业务流分析、假冒、旁路控制、授权侵犯、抵赖、计算机病毒、信息安全法律法规不完善等等，这些情况都会给信息窃取、信息破坏者以可趁之机。

失职公司是否有责任？

虽然罪犯已经落网，可未落实网络安全保护要求、没能及时发现升级漏洞的上海某科技有限公司又该承担什么责任呢？

该公司违反了《中华人民共和国网络安全法》第四十二条第二款之规定，不按规定采取技术措施和其他必要措施，未确保其收集的个人信息安全、导致信息泄露。根据《中华人民共和国网络安全法》规定，警方对上海某科技有限公司处 98 万元的罚款，直接负责该项目的主管人员孙某被处以 2 万元罚款。

温馨提醒

为了客户被盗刷的 6 万元，该公司和主管被罚了 100 万，企业真的得不偿失，这是血的教训！企业与其指望招到的所有员工都是君子，不如将安全措施落实到位。网络运营单位必须切实落实主体责任，依法开展公民个人信息保护工作，对于未按规定履行责任义务，造成公民个人信息泄露的，公安机关将依法追究责任。中国数据安全防护专家—亿赛通助力数据所有者实现信息资产的安全，并始终肩负使命为您提供有竞争力的数据资产安全解决方案和服务。

本文资讯来源于公安部网安局

谁在倒卖银行内部个人信息？

警方顺利破获大型贩卖公民信息案

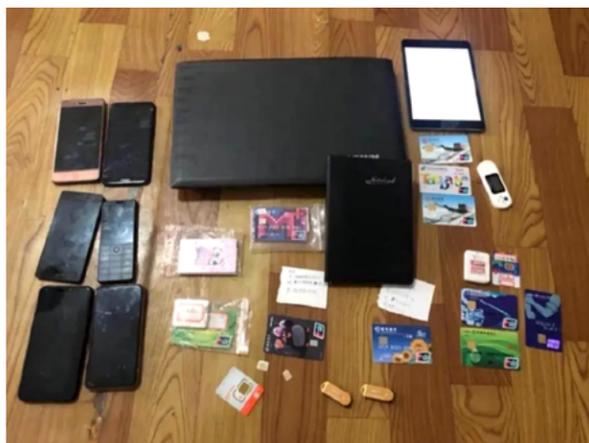
近日警方又立新功，破获了一起特大贩卖公民个人信息案，共抓获 26 名嫌疑人，涉案金额 2000 多万元。犯罪团伙通过现有的技术手段无法获取到如此大规模的公民个人信息，招揽银行内部的工作人员参与其中。

早在 2019 年 6 月，有人在网上通过 QQ 等通信工具公开出售银行卡相关信息，包括银行卡对应的卡主身份证号码、电话号码、余额甚至交易流水，引起了警方注意。男子称他发现与银行卡相关信息售价动辄几百元，且需求量很大，于是他转行当起了“信息贩子”。他根据客户需要查询的不同银行卡，对应不同的上线查询渠道，并以经济利益诱惑一名银行内部员工。



双方达成“合作”协议，银行员工每查询 1 条银行卡相关信息，即可获利 80~100 元不等的报酬。光凭这一黑色收入，年收入就超过 30 万元。

银行员工处在贩卖信息黑产业链的第一环，他联系中间商，中间商下面还有各种分销商，层层代理，形成一个以银行“内鬼”为源头、大量中间商为中介，通过网络勾结、贩卖银行卡的相关身份证、电话号码、余额、交易记录的网络犯罪团伙。由于层级很多，越到产业链的末端，信息的价格越高，从“内鬼”到销售末端，一条信息的价格可能翻上数倍。



除了内部员工泄密外，银行 APP 也成为被黑客“攻破”的突破口、非法盗取或入侵银行账户信息牟利。有公告显示，9 名团伙在两个月内利用“利用 APP 漏洞和使用抓包软件”，开设了 10000 余个银行三类账户，涉及国内多家银行。

此类型犯罪是利用了类似的 APP 技术漏洞，跳过银行开户所必须的“四要素”（即验证开户人姓名、手机号码、身份证号码以及绑定账户账号或卡号）验证，使系统误以为要对其本人的身份信息，最终完成开户。

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》显示，在对 133327 款金融行业 APP 进行扫描检测后发现，73.23% 存在不同程度的安全漏洞，70.22% 存在高危漏洞。平均每款金融行业 APP 存在 20.3 个安全漏洞，其中 6.7 个为高危漏洞。

近年来，监管机构已印发了一系列监管政策文件，要求银行保险机构认真贯彻落实个人信息保护方面的法律法规，加强客户隐私保护，对客户信息严格实行从采集到存储、销毁等全流程的制度化管理。政策方面国家已经在加强治理，同时专业的技术手段也必不可少，亿赛通独立研发的金融数据安全治理建设规划包含以下四个方面：

组织和架构的建设

传统网络安全均由 IT 部门负责，随着数据治理工作的深入开展，业务部门要深入参与数据资产梳理以及分级分类工作，因此原有的组织架构和项目模式无法支撑数据治理的深入开展，需要自上而下形成高层牵头、跨业务部门、数据全覆盖的组织架构。

制度和流程的建设

目前金融机构大多有较完整的安全规范，如分级分类规定，保密规定等，但一方面没有独立的数据安全规范，可执行性不强，另一方面缺乏技术监管手段，落地执行较难。在制度流程建设层面，可根据企业内部组织的特点分期进行建设。

技术工具的建设

传统的安全理念是“七分管理，三分技术”，随着数据量的指数级增长，仅仅依靠管理很难对数据进行全方位管控，而在实践中技术工具占据了越来越大的比重。传统的咨询项目交付物是大量的文档，而数据安全的项目真正能够落地执行离不开技术工具的管控。技术管控按照生命周期来分，可分为数据采集、数据传输、数据存储、数据使用、数据删除、数据销毁六个方面。根据数据分级分类进行安全环境和边界管控，保障数据的保密性、完整性和可用性。

人员能力的建设

传统安全人员的技术能力大多以网络安全和信息安全为基础，而在数据安全层面需要既懂业务，又懂数据安全体系的复合型人才，其核心能力包括数据安全管理能力、数据安全运营能力、数据安全技术能力及数据安全合规能力。对数据治理人员的培养和管理制度的宣贯需形成常态化机制，提高数据安全人员能力。

亿赛通根据金融业数据安全风险隐患并结合上级监管部门对金融行业的信息安全建设要求，提供全面的数据安全解决方案，相信如果从以上几点出发，从内部到边界所有敏感数据进行加密监管，不法份子也不会轻而易举的谋取暴利，有效杜绝损害客户信息安全的行为发生，维护消费者的权益。

新闻资讯来源于微博、江苏新闻

两会声音 | 安全问题如今刻不容缓……



今年，由于疫情的爆发，两会的召开比每年都要晚一些，政协会议已于昨日正式开幕。代表们就现今社会热点问题进行讨论……

建议一般商家不得收集个人生物敏感信息

针对“生物识别信息”设置专门的规定，即如无法律法规授权，即使在公民个人同意的情况下，一般商家、私人机构等也不得收集包含个人生物特征的敏感信息；建议采取国家特许或备案机制，未经行政许可或备案，不得从事此类信息收集或使用；建立敏感级评估机制，分级制定企业数据安全保护等级标准和要求。

建议出台《大数据法》维护数据权益

某代表建议从立法层面出台《大数据法》，对不同类型数据的采集、处理、存储、分析、使用、共享等各个环节制定专业清晰的法律法规，维护全链条数据权益，确保大数据安全可靠，保证大数据应用生态良好，发挥大数据最大作用和价值，体现国家治理的法治精神。

建议完善公民个人信息保护法律体系

个人信息保护法已被列入 2020 年的立法工作计划，加快推进立法进程对于当前统筹做好疫情防控和经济社会发展，不断提升人民群众的获得感、幸福感、安全感具有重大现实意义。

在个人信息保护法的制度设计中应该注意以下几个问题：

1. 在个人信息收集上，坚持最小化收集原则。可借助大数据、云计算、区块链等技术手段探索建立统一的公民个人信息平台，并由一个确定的主体负责收集、提供和保护。

2. 强化行政机关、事业单位等公共部门的自我规制义务。公共部门对于公民个人信息的收集往往具有强制性，且收集的范围更广、内容更为具体，故理应赋予其更为严格的个人信息保护义务。

3. 探索完善个人信息非损害类如骚扰电话、垃圾短信等侵权行为的救济途径。可尝试设置统一的个人信息保护执法机构，在个人信息保护法中完善个人信息侵权者的行政责任，赋予公民个人对非公共部门收集的个人信息具有自主删除的权利等。

此外，检察机关可考虑将此纳入公益诉讼范畴，解决好老百姓的痛点难点，比如骚扰电话、垃圾短信等问题，展现司法为民的基本宗旨。

建议做好疫情期间个人信息的“善后”处理

某政协委员表示，“疫情期间为防控需要，出入商超、写字楼等公共场所，扫码、填写个人信息成为常态。这导致掌握个人信息的主体众多，但在个人信息保护上差异很大，加强个人信息权保护和数据安全刻不容缓。”

目前个人信息保护法和数据安全法已经列入全国人大常委会立法规划。制定个人信息保护法时根据应用场景对个人信息进行分类分级保护。如：在突发公共卫生事件应急处置中，姓名、身份证号码、家庭住址、电话、定位数据、在线活动等与健康相关的信息，应“升格”为特殊类型信息。此外，基因数据、生物数据和健康数据等本身作为特殊类型信息，更应特别保护。

行政机关、公共机构的信息收集、使用和处理需要在个人信息保护法中加以规范。对基于数据关联分析的个人信息应加大监管力度，未经授权披露在传染病暴发期间收集的个人信息，可能会使个人面临包括污名化、歧视、暴力等很多风险，应依法提供足够的保护。

做好个人信息的“善后”处理是疫情防控的“必修课”。委员代表提议加快编制发布《重大传染病疫情突发公共卫生事件应急处置中个人信息保护管理指引》，明确有权收集和使用相关个人信息的指挥机构、执行机构，并明确相关工作启动条件和流程规范。并且将个人信息权保护纳入检察公益诉讼范围，特别是对在重大突发公共卫生事件应急处置中侵害众多公民个人信息权的行为，以及相关行政机关违法行使职权或不作为致使众多公民个人信息权被侵害的，应当提起公益诉讼。

两会大幕顺利开启，作为数据安全行业的先锋企业，亿赛通将持续关注国家政策，聆听社会大众的声音……

文章资讯来源于互联网

《个人信息安全规范》修订版已发布， 这些与你我息息相关



聚焦信息安全

新版《个人信息安全规范》上线

近日，国家标准《信息安全技术 个人信息安全规范》完成修订，将于2020年10月1日正式实施。此次《规范》着力解决《规范》实施以来出现的个人信息安全新问题，对部分原有内容进行完善，提升个人信息安全顽疾的治理效果。

1、新版《规范》解决社会关切问题

伴随移动互联网的迅猛发展，广大网民在享受移动互联网应用程序带来便利的同时，也饱受软件个人信息收集、使用乱象的困扰，通过功能捆绑等手段变相强迫用户授权，便是典型问题之一。

新版《规范》在个人信息收集部分增加了“多项业务功能的自主选择”的要求，在多项业务功能需收集用户个人信息的场景下，强调以业务功能作为基本单位，通过

规范初始征得用户授权同意、用户关闭或退出特定业务功能等内容，强化保障用户的自主选择，以此破题捆绑授权。

2、《规范》完善知情同意模式

《网络安全法》第四十一条要求“收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意”，确立我国个人信息保护收集、使用遵循“知情同意模式”。《规范》新增“根据个人信息主体要求签订和履行合同所必需的”、“与个人信息控制者履行法律法规规定的义务相关的”两种征得授权同意的例外情形。

一方面，个人信息控制者与信息主体存在合同关系并明确约定相关事项时，存在为订立或履行合同关系可能需要进行的个人信息收集、使用的情形，此时征得信息主体同意效率偏低而且可能与合同约定事项产生冲突；

另一方面，我国的法律监管要求，个人信息控制者也可

能因履行法律规定的义务进行必要的个人信息收集、使用，此时征得信息主体同意可能会有碍于实现其他法律法规意欲保护的公共利益。此外，为避免个人信息控制者泛化对于合同的理解，借由隐私政策滥用“根据个人信息主体要求签订和履行合同所必需的”例外事由，《规范》通过“注”的形式明确个人信息保护政策并不构成与个人信息主体之间所签订或履行的合同。

3、《规范》新增生物识别信息要求

生物识别信息包括基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等，具有唯一性和不可变更性，此前便作为个人敏感信息而在《规范》中受到更高层次的保护。《规范》实施后，指纹、人脸等生物识别信息被广泛用于身份识别、验证，刚刚过去的2019年，更被视为人脸识别商业化应用的元年，“刷脸”日益普遍。

《规范》修订关注产业发展趋势，在收集、存储和传输、共享、对外披露等环节，均着重强调了生物识别信息的安全要求。

1. 在收集环节要求生物识别信息的收集应当满足“单独告知”和“明示同意”的要求，强化收集生物识别信息时用户的知情与同意；

2. 在存储和传输环节，提出生物识别信息应当与身份信息分开存储、原则上不应存储原始生物识别信息、终端使用、及时删除等要求，通过落实生物识别信息存储和传输的最小化，从源头上降低生物识别信息使用可能引发的风险。

3. 在共享和对外披露环节，分别提出了生物识别信息原则上不应共享、转让，不应公开披露生物识别信息的要求，体现对生物识别信息使用的谨慎。

4、《规范》深化数据治理规则体系

数据商业潜能和价值的释放，离不开数据的聚合使用和畅通的数据流通渠道。我国《刑法》、《网络安全法》均禁止“非法向他人提供个人信息”，但并未明确在企业确因业务需要

进行个人信息流动时的数据治理规则。此次《规范》修订，除了补充、完善有关个人信息委托处理、共享、转让部分的要求外，也对企业进行数据汇聚融合提出相应的标准要求。

a. 需要个人信息控制者应遵守个人信息使用目的限制的要求，如超出收集个人信息时所声称的目的具有直接或合理关联的范围，应当再次征得信息主体的明示同意；

b. 如在汇聚融合中对个人信息进行加工处理产生的信息能够识别信息主体身份或者反映信息主体活动情况的，对其处理也应当遵循收集个人信息时获得的授权同意范围；

c. 对个人信息汇聚融合后的使用目的，还应当开展个人信息安全影响评估，并采取有效的个人信息保护措施。

信息安全国家政策 亿赛通鼎力支持

各种新技术的深入应用，带来个人信息保护的新场景、新问题，作为个人信息安全领域最为基础的国家标准，《规范》与时俱进为推进我国个人信息保护工作提供有益方案。随着信息安全问题日益突出，早已正式上升到国家安全战略高度，除不断提升软硬件自主研发水平外，此次新版《规范》，又将成为信息安全市场的一个爆点，两会期间，信息安全问题备受关注，国家和群众的重视让安全行业发展前景形势大好。亿赛通从事数据安全领域十七年，始终以专业、专注的态度为客户建设安全、高效的数据安全环境，为客户的数据保驾护航。

《规范》内容来源：中国信息通信研究院安全研究所

某大型装备集团与亿赛通强强联手， 打造中国工程机械行业安全标杆

工程部：蒋通龙 / 文



项目背景

近年来，信息安全的风险日益加大，国家和企业都对防范信息安全风险非常重视。国家信息化领导小组在 2003 年颁发的 27 号文件《关于加强信息安全保障工作的意见》，2017 年 6 月 1 日起实行的《中华人民共和国网络安全法》，2019 年 12 月 1 日起在全国范围内实施的《网络安全等级保护条例 2.0》；对我国信息安全保障工作做出原则性战略性的规定，要求坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全。

出于国家要求和企业自身业务的安全考虑，该集团迫切需要提高数据安全的保障水平。

本期项目建设目标：

以原有信息安全系统为框架，建设一套过程可控的文档安全管理系统；

对集团及所属 30 家分子公司涉及服务器、办公电脑、手机终端等进行安全管控，避免数据随意传播；

通过对设计网与管理网的文件（包括日常办公类、图形图像类、设计分析类和源码类文件）采取自动强制加密措施，实现数据安全预防；

通过安全系统的文档安全内容的权限设置，对复制、粘贴、打印、另存、截屏、删除、修改等操作进行控制，并记录相应日志，以便进行审计和追溯；

采取解密审批流程和文档流转外发的方式，同时结合水印技术，确保给第三方供应商、合作伙伴的文件安全可控；

实现亿赛通文档安全访问准入控制软件与业务系统集成，实现上传解密下载加密，不改变操作习惯。同时对非安装亿赛通加密客户端的电脑进行准入安全控制，不允许其访问内部的业务管理系统，如 PDM 与 GSS 等；

实现对系统审计日志（包括文件解密审计、文件打印审计、流程全文检索审计、违规操作预警等）的全程追溯。

项目成果

亿赛通为该集团完成部署后，企业内部实现内网一体化防护，保障敏感数据安全防护，员工在使用过程中，操作使用无感知。完美提升等级保护管理建设能力，并实现集团信息安全监控、合同等方面的要求。

长鑫存储技术有限公司



客户简介

2016年5月，长鑫存储的事业在“创新之都”——安徽合肥启动。作为一体化存储器制造商，公司专业从事动态随机存取存储芯片 (DRAM) 的设计、研发、生产和销售，目前已建成第一座 12 英寸晶圆厂并投产。DRAM 产品广泛应用于移动终端、电脑、服务器、人工智能、虚拟现实和物联网等领域，市场需求巨大并持续增长。长鑫存储将凭借值得信赖的产品和服务满足不断增长的市场需求，致力于成为技术领先与商业成功的半导体存储芯片公司，以存储科技赋能信息社会，改善人类生活。

需求背景

因长鑫存储发展及业务需要，各类包含大量重要信息的电子资料，如源代码、设计图纸、财务报表、技术文档等与公司知识产权相关的数据被高度共享，数据安全保护依赖某 DLP 产品，但其产品本身存在安全漏洞，这些核心数据关系到公司的生存发展以及商业竞争力，一旦泄密，将会给公司造成不可估量的损失。非核心数据安全保护层面的措施仅限于传统网络安全、存储冗余和文件服务器管理等层面，对于信息系统、业务平台、网络通讯、办公终端以及存储介质中的数据均以明文形式存在，在数据资产的使用、传输、保管、销毁的过程中存在较多安全风险，增加了信息安全管理工作的难度。

解决方案

根据长鑫存储现有情况，以及对文档安全管控的实际需求建立电子文档加密系统解决方案。

多密钥隔离：系统采用多密钥加密隔离方式，对不同类型的电子文档设置不同的密钥，密钥之间相互独立；

加解密中间件：提供加解密接口、外发接口给自研等业务系统，实现文件上传解密、下载加密、外发加密功能；通过策略方式实现指定业务系统 IP 的文件上传解密、下载加密功能；

策略模式切换：通过终端用户桌面悬浮窗口方式，用户自主切换策略模式，系统管理员在服务平台设置好策略模式对应密钥关系后，下发给终端用户。

加密锁图标显示：用户在同一台终端上，不同密钥加密的文件显示不同颜色加密锁图标，加密文件在网盘里的图标能够共存显示，一个系统可支持多种密钥锁图标；

密钥打印控制：用户在同一台终端上，不同密钥加密的文件可区分控制是否允许打印，不允许打印的加密文件，可申请打印审批流程，审批通过后方可打印。

项目成果

长鑫存储解决方案成功部署后，保障公司内部电子文档的使用安全，支持多种文档类型加密保护，防止用户通过剪切板拷贝、拖拽、另存为、截图等操作行为泄密；进行了文档权限管控，按照组织架构（部门、用户等）对文件进行授权管理，同时控制文档的使用权限及生命周期；通过对外发文档授权封装，保障数据在企业外部环境的使用安全；加密系统服务平台支持双机热备软件，提供高可用、安全性保障。