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

亿赛通 ESAFENET

ESAFENET

亿赛通企业月刊　　中国数据安全防护专家　　www.esafenet.com

3 月刊

2019 年共 11 期

心手相连·共赢未来 | 2019 年亿赛通渠道大会华南大区成功打响第一站！

心真大，Facebook 的又一重击！

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 刊首语

行业聚焦 INDUSTRY FOCUS

4-9 国内行业新闻

10-15 国外行业新闻

亿赛通动态 ESAFENET NEWS

16/17 心手相连·共赢未来 | 2019 年亿赛通渠道大会华南大区成功打响第一站！

亿赛通小贴士 ESAFENET PROMPT

18/19 【聚焦两会】安全问题迫在眉睫，个人信息保护法即将出台

20/21 315 痛批用户隐私泄露，数据安全该何去何从？

22/23 心真大，Facebook 的又一重击！

典型案例 TYPICAL CASES

24/25 防范敏感数据泄密，北汽研究总院携手亿赛通建立数据防泄露体系

26/27 亿赛通签约东风悦达起亚

共安全 享未来

阳春布德泽，万物生光辉。阳春三月，国内外数据安全圈依然“风起云涌”：京东白条账号大量泄露、抖音现金贷广告骗局、CITRIX 丢 6T 数据……从文字、图片到音频、视频，不断爆发数据采集、传输、存储各环节的恶性数据泄露事件。古人云，春江水暖鸭先知，数据泄露则是让中招的企业痛苦不堪。与其亡羊补牢，何不提前防范？

中国数据安全防护专家——亿赛通，为你数据安全保驾护航！

刊首语 PREFACE

国内

1、被外卖平台窃听、被地图定位住址，大数据下我们还有哪些隐私正在崩溃?

摘要：3 月 18 日，美团和饿了么这两款常用的外卖软件被曝窃听用户日常对话。在《IT 时报》记者长达 3 个月的测验下，他们发现：不管是安卓还是苹果手机，不管是美团还是饿了么，只要你在对话中无意识地提到某款食品，这些最常用的外卖软件总能及时地将对应的商家推送到你的首页，出现相关推荐的概率高达 60%-70%。

2、“白条”黑产追踪：京东账号遭大量泄露，黑市价高至每个千元

摘要：京东公司推出“白条”赊账功能后，尾随“白条”的各种犯罪层出不穷。3 月 16 日，网站报道了多名大学生冒充他人申请“京东白条”诈骗获刑，中国裁判文书网 140 余件刑事犯罪判例显示，“京东白条”的授信审核存在漏洞，有面签官收受好处、走过场。裁判文书披露，拥有“白条”功能的京东账户，遭大量泄露，并在黑市买卖。一个开通“白条”功能的京东账号，最高可以卖到 1000 元。更有犯罪分子抢劫手机时，逼问受害者的账号、密码，申请“京东白条”消费额度，用于购买黄金饰品。

3、5 亿条隐私打包售价 8 个比特币！个人信息泄露，远比你想象中严重！

摘要：2019 年的 315 晚会曝光了个人信息泄露的问题，让人触目惊心。据曝光，一种探针盒子可以利用无线网窃取用户个人信息。当用户手机在无线局域网处于打开状态时会向周围发出寻找无线网络的信号，一些公司将这种探针盒子放在商场、超市、便利店、写字楼等地，在用户毫不知情的情况下，搜集用户手机的 MAC 地址，再转换成手机号码。之后，这些公司再利用人工智能和大数据技术替代人工拨打骚扰电话和推销电话。

4、儿童隐私贩卖成数据泄露新趋势

摘要：近期，在暗网上出现了一波涉及未成年人的信息数据贩卖，具体来说是 1998 年到 2015 年出生的儿童的就诊记录，贩卖者声称他们收集的数据来自医院。

5、乱象难禁 征信 App 存泄露隐私隐患

摘要：第三方个人征信在生活场景中的普及应用，也催热了个人征信查询业务。但北京某记者注意到，在央行明确无授权的情况下，仍有不少 App 明确标注直连官方征信中心。另有部分 App 在输入银行卡账号和密码时才能获得查询权限。分析人士认为，这类 App 很有可能收集个人信息后交易给非法机构，衍生出新的“买卖”，导致信息泄露。

6、今年将推进立法的《数据安全法》，有哪些看点?

摘要：在 2018 年 9 月公布的“十三届全国人大常委会立法规划”中，《数据安全法》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”。在 2019 年十三届全国人大二次会议新闻发布会上，大会发言人张业遂表示在 2019 年将推进《数据安全法》立法工作。《数据安全法》的立法已经走上快车道。

7、2018 年近 50 亿条个人信息被泄露 内部漏洞远高于黑客攻击

摘要：与 2017 年相比，2018 年公开的数据泄露事件有所下降。数据泄露数量下降了三分之一，从 79 亿条下降到 50 亿条。据报告显示，2018 年公开披露的超过 6500 起数据泄露事件中，有三分之二来自商业部门。同时，政府部门占 13.9%，医疗部门占 13.4%，教育部门占 6.5%。数据显示，非常严重的数据泄露事情还将继续发生，而这对人们的个人隐私有着很大影响。

8、男子雇佣黑客窃取客户信息获刑

摘要：3 月 6 日，长沙市开福区人民法院审理了一起案件，被告人雇佣黑客非法窃取公司客户信息 20 万余条从中牟利，侵犯公民个人信息罪，被判处有期徒刑 3 年 6 个月，并处罚金人民币 15 万元。

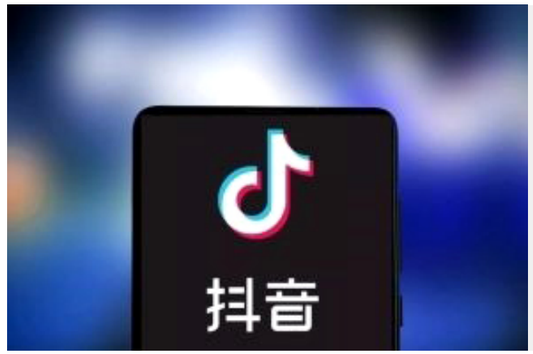
9、制作非法软件 网管变“神偷”！二男子涉嫌破坏计算机系统罪被批捕

摘要：一男子嫌网吧的网管收入太低，竟试图通过破解软件删除充值记录将钱据为己有，后又联合网友共同“研发”该软件用于售卖营利。近日，西青区检察院以该二人涉嫌破坏计算机系统罪依法批准逮捕。

10、贝贝网被诉泄露用户信息，宝妈遭遇诈骗集体维权

摘要：近期，有贝贝网用户向记者反映称，贝贝网存在严重的信息安全隐患，用户在贝贝网消费之后，包括个人姓名、电话、收货地址、消费金额以及交易时间等详细信息便遭到泄露；此后，更是有部分用户接连收到诈骗短信和诈骗电话，令人防不胜防。

11、抖音现金贷广告藏骗局：用户信息泄露、银行卡被强刷



摘要：因为在抖音上刷到了一款名为“米财”借款软件的广告，并在该 App 内首页醒目位置处下载了其推荐的另一款借钱 App“银开心”，网友在毫不知情的情况下遭遇个人隐私和财产的损失。

12、男子网购男性保健品后，惨遭电话轰炸十分尴尬，民警：网购要小心

摘要：某男子前一段时间在网上购买了一些保健品，在购买完之后，经常会接到一些推销保健品的陌生电话，每天有 30 多个电话给这名男子打来。随后在当地派出所报了警，经过警察对这件事情积极入手调查，最终发现，是因为该男子的个人信息暴露了，才导致有那么多人对他进行电话骚扰。随后民警便展开调查，最终抓获了该案件的嫌疑人。

国外

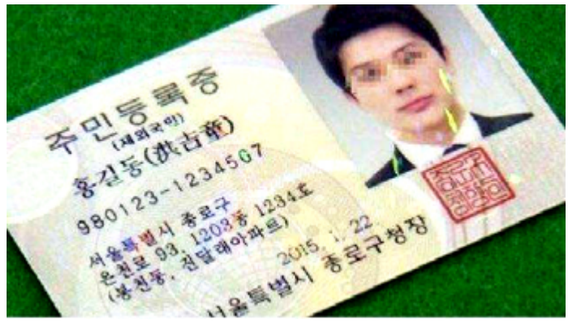
1、 黑客在暗网 Dream Market 出售 6 个网站 2700 万条数据泄露数据

摘要：黑客组织 Gnosticplayers 攻击了数 38 个热门网站，并将数据分成四次在暗网 Dream Market 上售卖，最近的一次数据泄露事件中， 包含来自 6 个热门网站的近 2700 万新用户记录 。

2、 新西兰运营商通过禁用 DNS 阻止访问含有枪击视频的网站

摘要：上周五在新西兰基督城发生了大规模枪击之后，为了限制视频传播，新西兰的多家互联网服务提供商（ISP）通过禁止 DNS 解析已经停止访问含有相关视频的网站。同时也有好奇的人通过搜索该视频，被跳转到钓鱼网站等，从而被黑客利用。

3、 韩国手机身份证 App 被曝存在严重安全漏洞

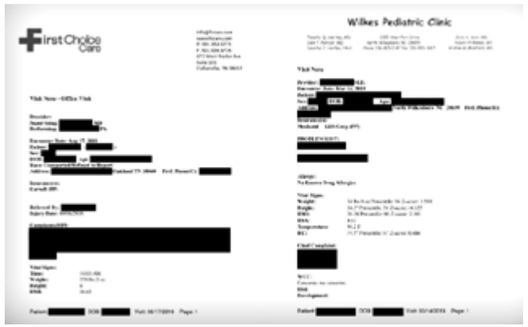


摘要：最近韩国一款“手机身份证”应用程序被曝出存在严重的安全漏洞。在这款“手机身份证”应用程序中，只要拍下身份证、驾驶证或学生证等证件的照片，就能保存在自己的账号中。然而，这款应用程序在保存证件照片时，不需要经过“本人验证”这一步骤，也就意味着，用户可以擅自把别人的证件照片保存在自己的账号中。这一安全漏洞便成了一些未成年人购买烟酒、出入不适宜场所的道具。

4、挪威海德鲁公司遭勒索软件攻击

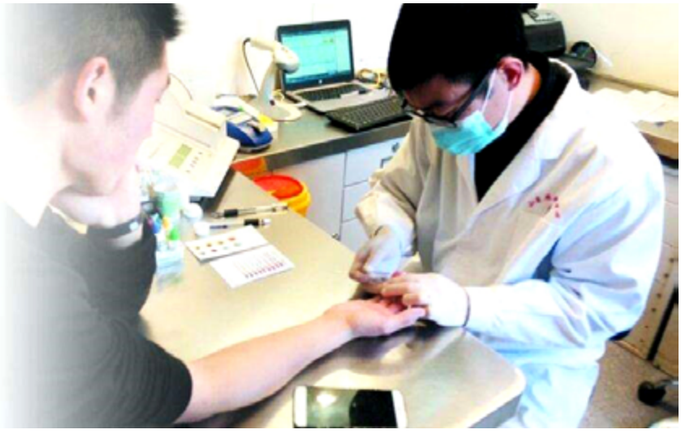
摘要：世界主要铝产品生产商挪威海德鲁公司（Norsk Hydro）遭遇勒索软件攻击，公司命令雇员关闭计算机，切换到手动模式。海德鲁公司称，恶意程序首先在周一晚上感染了美国地区的计算机，到周二晚上扩散到公司在其他地区的计算机。部分工厂临时关闭，部分必须继续运行的工厂则切换到手动模式。公司 3.5 万名雇员被要求关闭计算机，但允许使用手机和平板查看邮件。首席财务官 Eivind Kallevik 在新闻发布会上称，情况非常严重。

5、外媒：一家健康科技公司正在泄露大量医疗记录和处方



摘要：据外媒报道，一家健康科技公司在安全证书失效导致服务器没有密码后，每天泄漏数千张医生药方、医疗记录和处方。这家名不见经传的软件公司来自加利福尼亚州的 Meditab，自称是医院、医生办公室和药房领先的电子医疗记录软件制造商之一。该传真服务器没有得到妥善保护。自 2018 年 3 月创建以来，公开的传真服务器运行的 Elasticsearch 数据库拥有超过 600 万条记录。

6、新加坡 80 万多名献血者的个人信息泄露



摘要：最近新加坡发生了一系列数据泄露事件。例如，150 万名 SingHealth 病人的医疗信息被泄露，14,200 名艾滋病病毒感染者的个人信息被泄露。然而，最近新加坡发生了另一起重大数据泄露事件。这一次，由于第三方供应商未能妥善保护含有 808,201 名献血者个人信息的服务器，因此献血者的血型，身份证，体重和其他数据均被泄露。

7、外媒称 Gearbest 泄露数百万用户个人数据

摘要：3 月 17 日，亿邦动力获悉，国外安全研究人员发现，环球易购旗下自营网站 Gearbest 泄露了其平台数百万用户的个人资料和购物订单数据。该安全研究员 Noam Rotem 发现一台名为 Elasticsearch 服务器每周泄露数百万条交易记录，包括客户数据、订单和支付记录。且该服务器没有密码保护，任何人都可以进行数据搜索。

8、瑞士和澳大利亚的电子投票系统爆严重漏洞，可操纵选票

摘要：自 2004 年起，瑞士就一直在推行电子投票试点行动，瑞士邮政认为如今已开发出完全可经验证的可推广至全国范围内的系统。该项目将在 3 月 24 日结束，全球超过 3000 名黑客已经登记。一个名为“setuid(0)”的研究团队在代码中发现了大量漏洞，但瑞士邮政表示多数是“低危”级别。瑞士邮政发布漏洞奖励计划不久后，密码学专家 Sarah JamieLewis 和 Matthew Green 指出，加密函数中还存在一些潜在的严重漏洞。

9、户外品牌 Kathmandu 网店遭黑客攻击，客户交易信息泄露

摘要： 据外媒报道，在澳洲证券交易所上市的全球户外服饰和设备零售商 Kathmandu 披露，该公司在节后销售旺季遭遇数据泄露，客户的个人和支付信息被窃取。Kathmandu 在 Magento 电子商务平台上运营网上商店，过去几年，也曾有犯罪分子在未打补丁的服务器上攻击这个平台，并植入盗卡恶意软件。

10、供应商被黑，美国密歇根州 60 万居民医疗敏感信息或泄露

摘要：黑客利用勒索软件攻击了医疗服务公司 Wolverine Solutions Groups（WSG），而该公司和很多医院和医疗机构存在合作关系，导致该公司合作伙伴的用户数据遭到泄露，具体信息包括姓名、社会安全号码、地址和医疗信息等。

11、疑似伊朗黑客侵入企业软件巨头 Citrix 内网，窃取超 6TB 机密信息

摘要：企业软件巨头 Citrix 为企业、美国军方和多种美国政府机构提供服务，表示上周三通过 FBI 获悉黑客访问了其 IT 系统并盗走文件。伊朗黑客组织 IRIDIUM 从 Citrix 公司至少窃取了 6 TB 的敏感内部文件。据悉，从去年 12 月份到上周一期间，黑客盗走了邮件、蓝本和其它文档。黑客设法绕过多因素登录系统而侵入私有网络。

12、招聘网站数百万条敏感数据泄露，简历、身份证扫描件统统曝光

摘要：据外媒报道，美国乔治亚州杰克逊县的电脑遭到勒索软件攻击，导致政府活动陷入了瘫痪，政府决定向网络罪犯支付 40 万美元，换取文件解密密钥。这次袭击影响了全县所有部门的计算机系统。无线电通讯和电话不受影响，人们仍然可以拨打 911。

心手相连·共赢未来 | 2019 年亿赛通渠道大会华南大区成功打响第一站！

携手并进 风雨同舟

3 月 28 日，以“心手相连·共赢未来”为主题的 2019 年度亿赛通华南区渠道大会在广东惠州拉开帷幕。亿赛通华南大区的渠道伙伴齐聚一堂，在为期 3 天的会议中，亿赛通将与各位合作伙伴一同检验过去的成果，共同探讨数据安全市场的新动态，一起分享数据安全前沿解决方案，规划未来的发展方向。会中，亿赛通为参会者权威解读了数据安全的新方案。

在信息化、互联网时代浪潮的冲击下，数据安全市场需求愈加强烈，但同样行业竞争也更加激烈。那么，在如此激烈竞争的市场中，市场需求者究竟该如何选择数据安全服务商来保障企业内部的数据资产安全？而数据安全企业又该如何保持自我为客户提供优质的服务？本次大会正是从客户的真实需求、复杂混乱的市场竞争分析、与企业自身的状况出发，共同探讨企业如何保持自我继续在 2019 年为整个数据安全市场提供服务。

面对客户，亿赛通严格要求每一个员工，同时，专业高效的研发技术人员与 7*24 小时的售后服务体系完美融合，有效提升产品质量及客户业务体验。先进的产品创新理念，完善的渠道政策为合作伙伴提供了新的市场增长方向，坚定了合作伙伴共赢未来的信心。亿赛通专业的数据安全技术结合渠道伙伴对行业的深度理解，必将在数据安全领域的建设中带来更广阔的发展空间。2019 年，企业将继续深化数据安全生态圈合作，全新升级合作伙伴计划，扩大与渠道伙伴的合作共建。

合作共赢 坚持自我

在同行业中，我们坚持持续创新的精神、专业的态度、踏实的步伐，认真的为每一位客户提供周到的服务，从而在优质企业文化价值的深层耕植下，研发出过硬的产品，丰富的数据安全解决方案，从根源上保护客户的数据安全。

今后，亿赛通在华南区将会继续拓宽渠道建设，让品牌打响每一个角落，公司在为自身创造价值的同时，也是对中国数据安全行业做出的一个巨大贡献，能够引导市场竞争规则更加有序化，并给客户提供真挚的服务，让千千万万的企业资产安全无泄露。

【聚焦两会】安全问题迫在眉睫，个人信息保护法即将出台

全国两会重点关注个人信息保护问题

近日，十三届人大二次会议新闻发布会顺利召开，个人信息安全成为会议主要讨论议题，牵动着广大网友的心。随着网络信息技术和数字经济的快速发展，因个人信息不当收集、滥用、泄露，导致公民权益受到侵害的事件时有发生。个人信息安全立法刻不容缓，通过立法加强个人信息保护已成为保护公民隐私和生命财产安全、规范网络健康有序发展的必然要求。

事实上，我国已经有多部法律、法规、规章涉及个人信息保护。比如刑法、民法总则、消费者权益保护法、网络安全法、电子商务法等，都作出了相关的规定。但是从总体上看，呈现分散立法状态，所以需要根据形势的发展，制定有针对性的专门法律来加以规范，形成合力。全国人大常委会已将制定个人信息保护法列入本届立法规划，相关部门正在抓紧研究和起草，争取早日出台。

为什么个人信息安全要立法?

随着信息技术的高速发展，个人信息的搜集变得越来越容易。对信息的不当使用或予以公开会给个人造成财产、精神上的损失。因此，对个人隐私权的保护不能只停留在所谓独处权的保护上，而应该朝着保护个人信息的方向发展。隐私权已经从传统的“个人生活安宁不受干扰”的消极权利演变为现代的具有积极意义的“信息隐私权”。现阶段就保护公民的个人信息作出规定，无疑对于那些非法出售、提供或者以窃取、收买等方式非法获取公民信息的不法之徒是一种威慑。同时，我国以修改刑法的方式介入个人信息保护，表明了国家对公民个人信息保护重视的程度，同时也证实了国家对公民个人信息保护的力度。

个人信息保护法重点任务是什么?

个人信息保护法的制订将更全面更完整地保护网络上的个人隐私和信息，一是对政府部门利用公权力泄露个人信息应当加以重点规制；二是对一些大众服务类企业，诸如金融、电信、交通、教育、医疗等单位，对客户信息的保护应当作出严格的规定。同时，在个人信息保护法即将出台，保护个人的隐私的基本精神得以确立的情况下，互联网企业要加强自律，遵守基本的道德规范和网络秩序，增强网络企业公民的社会责任感。法规和自律相结合，一个适合国情、相对完善的个人信息保护体系就不再遥远。

亿赛通以成熟产品及解决方案鼎力支持个人信息保护

亿赛通从事数据安全防护领域十六年，已发展成为国内数据安全、网络安全及安全服务三大业务供应商，以上百项知识产权涵盖了包括：终端、网络、存储、审计等多个方面的几十个数据安全软硬件产品，坚持为广大客户提供核心技术保障。对于个人信息保护法的出台，亿赛通鼎力支持国家政策，并且努力从技术方面持续为大家的信息安全保驾护航，携手国家政策共同致力于建设安全、高效、文明、和谐的信息安全环境。

315 痛批用户隐私泄露，数据安全该何去何从?

一年一度的“3·15”国际消费者权益日如期而至，其实，连续几年，315 晚会的重点都不只在打假维权，“信息泄露问题”也早已成为 315 关注的焦点！

据有关数据统计，截至 2018 年 12 月，我国网民规模达 8.29 亿，但是仅一年内，垃圾信息、诈骗信息、个人信息泄露等事件层出不穷。AcFun900 万条用户数据外泄；前程无忧的 195 万条用户求职简历泄露；圆通快递 10 亿条快递数据被售卖；顺丰快递 3 亿用户数据被兜售；5 亿条华住旗下酒店客户开房数据被出售；万豪集团 5 亿名客人的信息被泄露 ... ... 网站、酒店、快递公司等都成为信息泄露的源头，以上数据，足以看出个人信息安全问题的严重性。

今年 315 晚会更是点名曝光高科技灰色产业链，企业通过智能机器人打出大量骚扰电话；还有企业通过 " 探针盒子 " 来搜集附近用户的电话，从 APP 中获取用户隐私信息。

16 日下午，工信部责令基础电信企业即刻关停企业拨打骚扰电话的语音专线，停止违规号码透传，加强通信资源规范管理，同时对报道中涉及的呼叫中心企业进行核查处理。针对报道中手机 APP 收集个人信息问题，工信部要求腾讯、百度、华为、小米、OPPO、Vivo、360 等国内主要应用商店全面下架 " 社保掌上通 "APP；并对 " 社保掌上通 " 手机 APP 的责任主体公司进行核查处理。此外，工信部还将对同类 APP 进行排查检测。

《消费者权益保护法》规定，经营者及其工作人员对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。企业没有尽到安全管理责任，应承担相应的民事责任，赔偿用户损失。

亿赛通让数据更安全

消费者下载 APP 或购买产品服务时会填写个人敏感数据，如身份信息、手机号码、家庭住址等，这些数据被存储到应用系统后台后，企业必须承担安全管理责任。由于数据保护措施不到位、审核流程不完善，极易给不法分子可趁之机，导致企业“内鬼”信息泄露事件。

作为数据安全领域一流的解决方案供应商，亿赛通致力于党政军、设计制造、金融证券、能源、金融证券、集团企业、运营商等行业提供专业的数据安全产品及服务。企业肩负着“保护数据所有者的信息资产安全”的使命，为数万家企业及 400 余万终端用户铸就了坚不可摧的安全盾牌。

除从内网层面为用户提供文档加密、数据安全智能管理平台（DSIP）等数据安全产品外，亿赛通还用户提供数据安全咨询服务，帮助企业分析安全隐患，有效规避风险，全方位保障用户数据安全。未来，亿赛通将继续创新，为各企事业单位数据安全保驾护航！

心真大，Facebook 的又一重击！

大数据时代，我们的个人数据，被各大互联网公司奉若至宝，为了更好的帮你“剁手”，巨头爸爸们想尽办法把你“扒的干干净净”。曾经的社交行业巨头 Facebook 如今丑闻缠身，近日又遭重击……

危机公关难以挽回的泄露困局

自 2018 年 3 月以来，Facebook 中将近 8700 万名用户的个人信息遭到数据公司泄露；同年 9 月，该平台再次声明，因为平台中存在的安全漏洞导致了黑客入侵，再次导致将近 9000 万人的信息受到影响，其中 5000 万用户的数据遭到泄露；之后在 12 月，Facebook 因软件中存在的漏洞可能会导致 6800 万用户的私人照片泄露。

时至今日，仅过 3 个月，Facebook 又被爆出存储了大量没有加密的用户帐户密码。账户信息曝光的用户具体人数还不确定，估计在 2-6 亿人之间。这些账户密码可以作为纯文本，给 2 万多名公司员工查看。

由于不断爆发的隐私和安全丑闻，Facebook 受到了严格的审查。这些丑闻引发了客户的批评，以及多家监管机构 (尤其是欧盟 (EU) 的质询和罚款。按照《通用数据保护条例》规定，Facebook 的最新事件无疑将触发审查，因为该条例要求相关公司在 72 小时内向受隐私泄露影响的人发布通知，并要求公司安全存储密码。对于如何准确定义“适当的安全级别”，这项法律有点含混不清，但欧盟委员会可能会认为，存储在内部并可供大量员工使用的纯文本密码可能并不符合标准。

安全问题急需根治

Facebook 多次事件给网民敲响了警钟，用户数据作为平台掌握的重要资源，已经成为互联网企业的核心资源。社交平台中出现的数据泄露事件揭示出互联网企业背后的潜在利益逻辑，反观国内网站和 App 软件，在用户数据方面同样存在着类似的问题：视频网站 A 站及交友软件陌陌均曾爆出泄露情况；在泄露信息之外，过度收集用户信息，同样在国内的 App 以及网站中不断出现。

面对这种情况，有效地解决措施往往会是政府监管及政策法规。刚刚结束的两会及 315 国际消费者权益日均涉及数据安全领域，政府明确表示大力推进《数据安全法》的立法与实施；工信部此前也针对 APP 过度收集个人信息情况进行整改。

保护数据安全，加强技术投入

安全领域的竞争是当前国家间重要的竞争领域之一。各国普遍重视安全领域的立法，对关键信息基础设施保护、个人信息安全保护、数据安全管理等方面事项进行法律规定。在与其他国家进行合作和竞争过程中，如何保障国民和企业利益是各国政府高度重视的问题。

保护数据安全，不仅需要政策的支持，更需要结合技术共同防范。讲到技术防护层面，亿赛通详细的数据安全解决方案，以“疏、堵、管、控”的理念为方针，综合互联网、大数据、智能技术、云安全、移动电话网、固话网络等主流通信渠道的信息审计功能于一身，采用先进的行为、内容、模式、声纹等识别技术，结合智能的信息干预等手段，对不良信息传播、网络犯罪等进行有效管控。有效支撑国家信息空间管理业务，提升国家公共安全工作的发现、管理能力与处理效率，未来也将继续为国家安全贡献重要技术力量。

防范敏感数据泄密，北汽研究总院携手亿赛通建立数据防泄露体系

关于北汽研究总院

北京汽车研究总院有限公司（简称：北京汽车研究总院）是北京汽车工业控股有限责任公司为实现北京汽车工业集团化发展战略目标、构筑自主研发平台、提升自主创新能力、打造北京汽车自主品牌而出资组建的独立法人实体。主要从事汽车整车 (包括乘用车、越野车) 关键零部件的研发及混合动力等新技术的研究。北京汽车研究总院设立乘用车工程院和越野车工程院两个工程院，研究总院及两个工程院共设有造型部、新技术研究部、试制试验部、CAE 技术部等 21 个部，69 个室。

需求背景

北汽研究院内部存有企业大量重要信息，如设计文档、源代码数据、图纸文档、技术资料、项目方案、招投标书、客户与商务资料、财务信息、人事档案等都散布在员工的电脑、院内的应用服务器或流转于网络之中，因此给北汽研究院的信息安全带来了巨大的隐患。

解决方案

亿赛通为北汽研究总院部署电子文档安全管理系统：

1、核心数据透明保护：

1）研发设计部文件保存时自动强制加密，同时支持文档自动全盘初始化加密；

2）加密的文件在同一动态加解密区域内（同一部门内或部门之间）可以不受限制使用，文件非法流转到企业外部，将无法使用；

3）加密的文件如果要给区域外部人员使用，必须通过有解密权限的人员专岗通过出口解密；

4）动态加解密区域员工出差时，将通过终端脱机管理控制进行离线办公。

2、从密文到明文

非接触性解密申请明文发布方案，通过非接触性解密申请 (自动解密和手动解密) 提交给审批员，审批员通过审批之后，采用自动解密方式的就可以直接实现明文发送；解密审批后明文发布方案，通过审批员对待发布信息进行在线审批后自动完成解密。

3、移动办公

1）离线审批解决方案，通过审批员对离线用户进行在线审批后，申请用户可实现离线限定时长安全使用；

2）通过离线补时功能，可以实现离线用户逾期无法连接服务器时的离线补时支持。

4、准入网关

通过安全网关设备过滤，实现密文下载、明文上传解决方案。

项目成果

通过在北汽研究院全面部署实施数据防泄密系统，只有授权用户权限才能访问到敏感数据，且所有到达终端的敏感数据都进行了加密。数据使用和解密都经过规范的流程，极大程度地保护了敏感数据的安全，实现了数据审计的可追溯，配合相应的制度管理，达到项目建设目标。

亿赛通签约东风悦达起亚

企业简介

东风悦达起亚汽车成立于 1944 年，至今已走过了 63 个年头，已在全国范围内 29 个大中城市拥有 50 多个销售及售后服务网点。目前，公司向中国市场推出 OPIRUS（欧菲莱斯），SORENTO（索兰托），SPORTAGE（狮跑），CARENS（新佳乐）和 VQ（威客）等 5 款车型。每一款都以出众的品质和超凡的价值得到了中国消费者的赞誉和青睐，在各类车型评比中荣膺大奖。据统计，起亚进口整车的数量每年以平均 30%的比例增长。

典型案例 TYPICAL CASES

需求背景

悦达起亚汽车属于中韩合资企业，韩国本土已经上过一款韩国的加密软件，但是在中国他们的使用方式不适合他们的办公操作习惯。所以为了迎合韩国防泄密的要求，中国总部盐城要求全集团部署加密软件。并且亿赛通的加密软件和韩国的加密软件能做到完美结合，不发生冲突。

解决方案

亿赛通产品有国际化版本，能够和客户的域做集成。该产品实现了企业内部电子文件的加密存储。无论是由人工生产还是由应用系统生成的，只要写在磁盘上就是加密形式；另外，只有被系统授权许可，才可使用这些加密的文件，如未经合法许可将加密文件数据体带走，加密文件内容将不能够被正常打开，从而确保文件内容不会因为文件数据体扩散而扩散。

项目成果

完美支持客户韩文操作系统，并且和韩国本地的加密软件完美结合，两地的密文互通畅通无阻，客户非常满意。