

盗号衍生黑产业链,年牟利超百亿 2017网络安全生态峰会共议新安全挑战

立体联动,精准治理,打造安全金融生态

盗号所衍生的黑产业链年获利超百亿元。在7月26日—27日的2017年网络安全生态峰会(简称ISS)上,电商生态安全联盟发布了《电子商务生态安全白皮书》,首次披露了中国电商的生态安全状况。数据泄露、账号被盗、敲诈勒索等风险与消费者息息相关。

2017 ISS聚焦新型网络犯罪类型、解剖新型犯罪手段,共话中国网络“新安全”,联动社会各行业、各领域,“共担当”新业态下的网络安全责任,并通过社会各行业、各学术领域的携手和聚力,让科技赋能社会治理,推动安全生态共建,为互联网产业的健康发展赋予更多能量与动力。

同时,峰会还带来了全球最前沿的技术、科技,促进国内安全技术的发展与交流。

■记者 黄文成 实习生 寻颖 石璇

新技术革命,将坏的变成好的

阿里巴巴集团秘书长、风险委员会主席 邵晓锋



大数据而产生一些新的行业在迅速的发展过程当中,也伴随而产生了大量的黑灰产成形、规模几百亿、上千亿的黑灰产业正在不断的形成,最近几年经过司法的体系、执法机构以及相关部门的共同努力,包括各大公司、各大机构、各专业人员的努力下,这一些势头有所遏止,但是今天形势还依然非常严峻。

如果没有一个良好的互联网大数据形态,新的生态环境,所有的新的产业发展、社会的发展都会受到非常巨大的影响。

新安全其实就是基于互联网大数据新的信息技术革命背景下,所有的能力提升、机制的提升、技术的提升,把所有的单点防御、被动防御,变成更多的联合防御、联合打击、主动防御。甚至于形成一个企业政府、公民个人、专业机构、全体立体联动的整个对互联网安全生态的构建体系。包括对很多司法环境、司法体系不断的推动和深化,形成全方位的网络安全生态的体系。

大数据技术最近几年越来越多地被各行各业所接受。其实我觉得这一次以互联网技术为基础的这样一个新的信息技术革命正进入到一个关键的时期。

但是我们在和很多机构甚至不同的国家交流过程当中听到一个非常惊人的信息,所有的主要国家涉及互联网犯罪都至少以30%以上的速度在增长。国内各种系统攻击、窃取信息、各种利用互联网平台进行敲诈、偷盗、勒索、欺诈等的各种犯罪行为,也在迅速的增长。

很多互联网基于互联网

发挥纽带作用,落实国家政策

中央网信办网络安全协调局副局长 胡啸



信息安全;要科学平衡信息网络数据的依法有序,自由流动和数据安全保护之间的关系,采取措施切实保护,重要数据的安全,做到既能保护重要数据和个人信息的安全,又要能够促进数据的依法有序自由流动;坚持网络安全为人民、网络安全靠人民,切实保护个人信息安全;要发挥好联盟的桥梁纽带作用,加强行业自律。

希望我们的企业能够参与到国家的政策和标准的制定,尤其是在贯彻落实这些政策和标准的过程中要发挥作用,引导一些企业按照政策和标准的要求保护好系统和关键基础设施,保护好重要数据的安全,保护好公民的个人信息。

最近一段时期很多关键基础设施遭受网络攻击,一些重要的国家相关的基础数据和个人信息泄露的事件不断的发生,给国家的安全和公民的利益带来了严重的损害。

因此我们要坚持技术管理和网络安全并重,确保关键信息、基础设施、重要系统的

网络安全升级,护航新金融

蚂蚁金服集团CEO 井贤栋



这几年科技和金融的融合正在不断的深化,一个新金融的生态正在形成。用户、人群扩大了;开始以用户为中心重新组织服务方式,向用户提供更加个性化的服务;数字化金融正在成为全球性趋势。所以安全是新金融可持续发展的一个基石。只有一个更好的安全体系,才能有新金融的未来。

同时也给安全带来了许多新的挑战,要更加注重安全和体验的平衡:线上线下的融合、数据安全、信息安全、个人隐私保护的重要性、灰黑产业链的技术升级再加上新金融是一个完整的体系,环环相扣。

新形势下的网络安全需在三方面升级:一个是技术驱动,今天由数字化金融随时随地、7×24小时向全球每一个消费者、向每一个普通大众提供金融服务;第二个是叫生态共建,跟清华大学也展开了联合实验室,蚂蚁金服也和同行在合作,并开始配合执法部门,从传统打击开始向整个数字打击升级;第三个是要责任担当,我们推支付宝支付,把安全看作生命线,不辜负用户所托,不辜负用户的信任,给到每一位用户最好的安全保护。

面向新金融时代在新的环境下整个数字金融的未来,我们希望技术驱动、生态共建、责任担当,让我们共同推进网络安全进行升级,护航新金融,给每一个用户更安全的金融环境。



当前网络黑产所带来的安全挑战愈加严峻,对抗网络黑产不能单纯依赖技术手段“一刀切”,而应该从“技术升级、人性服务、可信保障”三个维度建立行业服务准则,以此有效提升黑产对抗效率。在黑产对抗方面,腾讯安全基于过去十余年的经验和技

大数据网络治理,充分利用技术

公安部网络安全保卫局副局长 钟忠



当前大数据已经成为全球治理的很重要的工具,在互联网安全生态治理当中如何推动大数据深度的应用,也是我们应该抓准和加强的方向。同时,大数据在网络治理中突出的作用,需要我们利用大数据扁平化、快捷性,实时互动这样一个条件打造精准治理、多方协同的这样一个互联网治理

理新的模式。

建设一个良好的网络生态环境,核心目的是要对我们网络社会每一个领域、每一个参与者,对它的发展提供有效的支撑和保障。这一目标实现中,需要不断完善我们大数据的基础设施,注重大数据的安全。

这需要全面的贯彻落实《网络安全法》,充分利用多种技术多种措施,履行网络安全保护的责任,营造一个安全、有序的网络环境;其次要运用大数据思维,提升精准打击犯罪的能力,继续严打整治侵犯个人信息犯罪,打击黑客攻击;积极推进网上打防管控一体化建设,鼓励和支持把我们大数据、云计算、物联网等等先进网络技术运用到网络安全上。

技术全面创新,“四心”成衡量标准

阿里巴巴集团首席风险官 刘振飞



互联网已经成了连接全世界、连接我们所有业务场景的业务设施。基于对互联网的新认识,我们要有一个新的互联网安全观,如何衡量互联网安全做的好不好,要用四心来衡量:让消费者安心,让互联网经营者让省心,让整个黑灰产业胆战惊心,让我们监管执法人员放心。而我们同时还需要从技术能力、数据、合作、创新四个方面加强。

比如说在阿里巴巴的发展

过程中,除了底层基于数据、安全平台之外,同时认为还要做监管机构和学习者的密切合作,做好线上线下的连通群防群策与生态和合作伙伴安全的联盟,但是有各种各样的合作伙伴,他们安全没做好我们的平台都是不安全的,在实践中有几个点非常关键,第一点就是数据预警,第二是个人的防控,最后是做好蓝军工作。

大数据风控、出特云保护平台、电商生态安全联盟和打拐神器——团圆,这些重大事件都说明了风险的危害性。

近两年来,阿里巴巴一直在与整个生态加强合作,通过技术创新、技术数据创新、通过监管创新,一起努力共同打造整个今天生活依赖的互联网的业务技术安全,一起努力把这项技术做得更好,最终所有人都是参与者也是受益者。

开放平台,共建互联网安全新生态

腾讯副总裁 丁珂

累,已经在行业内形成了一套完备的人性化服务体系。

安全不仅是腾讯公司的核心战略,更是腾讯公司践行社会责任的重要体现,腾讯将坚持开放、合作、共享的理念,推动中国互联网安全新生态的建立。

在联合行业合作伙伴共同打击网络黑产的同时,腾讯安全不断向国内外持续输出安全实力,2016年腾讯安全联合实验室发现谷歌、微软、苹果等国际厂商共计269个漏洞,位居国内第一。腾讯安全联合实验室旗下科恩实验室以“全球首次远程无物理接触方式破解特斯拉汽车”的研究成果,

成为2016年唯一一支获得“特斯拉安全研究名人堂”的团队。另外,腾讯安全还是苹果iOS11、Safari系统独家安全合作伙伴。

另外,在向行业输出安全实力的同时,腾讯安全还利用自身优势打造网络安全人才培养闭环,为国内安全行业持续“造血”。腾讯安全发起并举办了腾讯信息安全争霸赛(TCTF),由腾讯安全联合实验室7大掌门人和国内数十位资深网络安全老师组成的明星导师团,为通过比赛选拔的学生进行指导,并将优秀选手输送到国际赛场,促进实战人才的培养。