国家网络安全宣传周 China Cybersecurity Week

2018年国家网络安全宣传周 上海地区活动

9月17日,国家网络安全宣传周上海地区重点活动之一的网络安全高峰论坛在复旦大学举行。行业专家、高校专家、产业界代表就网络安全国际形式、产业发展、技术研发、人才培养等议题进行交流讨论。

随着全球信息化的快速发展,互联网新技术已经渗透融入到社会生活各个领域,网络日益成为人们生存活动中不可或缺的空气和水。但随着互联网应用的爆发式增长,也暴露出越来越多的网络安全风险,网络安全不仅是互联网技术问题,更是包含国家安全、社会安全、基础设施安全、人身安全等大安全的概念。

上海作为全面开放的现代化国际大都市,随着智慧城市的建设和"互联网+"行动的深入推进,互联网与经济社会的融合程度越来越高,网络和信息系统在城市运行中的全局性、基础性的地位也日益凸显,金融、能源、电力、通信、交通等基础设施领域的关键信息更是成为经济社会和城市安全运行的神经中枢。

近年来,杨浦区在这一宏观背景下,不断加快推进"三区一基地"建设,有力推动了杨浦互联网产业发展,人工智能、区块链、大数据、智能制造、云计算、物联网已经成为杨浦聚焦的产业发展方向。在产业发展同时,进一步加强网络态势感知系统建设,进一步提升全区网络安全水平。

一个基于互联网的第五空间,已经真实地呈现在我们面前。如何构筑网络屏障,如何提升网络安全的意识,如何化解安全和威胁,成为论坛上专家和平台共同聚焦的问题。 ■成佳佳 朱良城

2018年国家网络安全宣传周网络安全高峰论坛——

聚焦网络安全 营造良好网络环境

沈逸:全球网络安全需要多方合作治理

复旦大学副教授沈逸在谈及全球网络安全时表示:"当今世界,没有任何一个单一国家能够从大规模网络攻击中幸免遇难。"

在他看来,当国家级网络武器与技术扩散之后,一旦受害国将此视作政府行为进行反击,就可能引发一场实体冲突甚至局部战争。如何预防这种威胁,以及如何防止这种威胁由网络空间向非网络空间蔓延,对于从事网络安全行业的从业者来说是全新挑战。

沈逸指出,全球化环境下,任何一项关键基础设施,从生产、引进、制造到部署都具备全球化成分。"在此过程中,除非我们具备一条可信供应链,否则我们将无法保障各个国家关键安全利益得到有效保障。"此外,信息操控能力扩散与新型政治战以及战略数据资源的识别与竞争性管控,都是全球网络空间面临的新威胁。

沈逸认为,全球网络空间安全问题的解决需要重大战略创新。从中国进入互联网以来,基于自身发展的经验和需求,提出了超越传统意义上的多边主义,和多利益相关方探讨多方合作治理模式,在全球范围内表现出独特优势,"多方合作治理模式可以确保各个行为体找到自己恰如其分的位置,并且能为改善全球网络空间态势、提升治理绩效做出独特的贡献,最终形成真正意义上造福世界人民的治理方案。"

蒋瞳:银行业网络安全技术应走向主动防御

浦发银行科技部总经理蒋瞳认为,银行业作为高度依赖信息技术的行业,同样面临着巨大的信息安全挑战。近年来,银行业遭受的各类攻击都以追求经济利益为主,很多是为了获取银行数据,部分全球勒索软件的攻击使得数以百万计的用户资料被加密破坏。依托互联网分工协作进行网络攻击已形成常态。

蒋瞳表示,银行是数据密集的行业,数据资产众多,大数据应用要求广泛进行共享,也加大了信息安全的防护难度。此外,越来越多系统跟互联网紧密相连,跨界合作过程中,与第三方机构的互联互通更加普遍,因此被攻击面不断扩大,增加了系统被攻击、破坏的可能性。

在谈及银行业如何应对网络风险时,蒋瞳表示,与一般的被动防护不同,浦发银行从安全治理、安全技术、安全运营、以及安全管理四个角度,覆盖各个安全管理领域,纵向实现业务与技术的安全融合,横向扩展到所有信息资产。

"我们的信息资产相当庞大,当这些资产遇到攻击的时候,如果有一点没有更新掉,都会在整个系统蔓延。"蒋瞳表示,为此,浦发银行正着力推进全面安全管理三年行动计划,希望通过三年时间使安全技术走向主动防御,安全运营实现智能化安全防护,应急处置达到先进水平,有效保证信息科技风险可控和业务拓展安全,为数字化战略转型构建坚实的安全保障。

胡绍勇:推进数据安全分类分级保护制度

观安信息CEO胡绍勇,在论坛上发表了《大数据时代下的关键信息基础设施安全》的演讲。

胡绍勇表示,在当前数据时代,云计算、大数据、移动互联等新技术层出不穷,传统网络的边界逐渐泛化,纯粹从传统网络控制的角度做安全防护,难度越来越高。近年来,一些互联网企业就提出了新型的边界防护的理念。

面对数据集中带来的数据风险,整个安全防护思路就要做相应转变,首先要对应用接入进行安全防护,包括防控的权限管理;其次是基于数据安全防护,包括对数据分级分类,以及对数据的防控和脱敏进行安排;最后是针对大数据平台的安全防洪,包括账号管理、统一认证、权限管理、访问控制,以及运维审计进行相应的安全需求防护。

胡绍勇认为,保证数据安全首先要建立数据分类分级保护制度。制订分级分类的企业策略之后,对当前企业内部的数据进行梳理,对敏感数据进行分布监测,针对不同的敏感数据级别,制定相应的数据保护的策略,对各技术平台存放的文本数据进行发现和标识,方便后续安全控制,也便于对相应的敏感数据进行细粒度的管控。

宗泽:全民参与共建网络安全生态

上海优刻得信息科技有限公司CSO宗泽认为,如今网络安全风险是除自然灾害以外的最大风险,大型的网络安全事件对全球范围内的网络安全威胁日益突出。"以Facebook泄露5000万用户数为例,一度造成该公司市值下跌1000亿美元;2017年,影响全球的Wannacry勒索病毒,至少有150个国家遭受了攻击,受害的电脑超过了23万台。"

为应对新情况、新态势,近来网络信息安全方面的监管日益严厉。《中华人民共和国网络安全法》规定了企业作为网络运营者和关键信息基础设施运营者必须遵守的法律准则和义务,刑法修正案中增设了出售、非法提供公民个人信息罪和非法获取公民个人信息罪,明确了拒不履行公民个人信息安全管理义务行为的处罚。对此,宗泽表示:"我们可以看到,不管是国家之间,还是从整个全球的经营环境来看,网络安全会成为影响到大家生活的一个非常重要的问题。"

此外,宗泽还强调,网络安全重在全民参与,希望有更多人、更多企业、更多院校参与进来,共建网络安全生态。