编辑 张绪旺 美编 代小杰 责校 李月 电话:64101906 shangbaoIT@163.com

腾讯CSS峰会:

构建未来安全生态亟待三大举措

2016年11月9日,第二届中国互联网安全领袖峰会(Cyber Security Summit,简称CSS)举行,主题为“智慧安全 连接赋能”,包括高通、微软、谷歌、英特尔等顶尖科技企业在内的500家全球企业代表参会。中国量子通讯第一人潘建伟、腾讯公司副总裁丁珂、高通副总裁Alex Gantman等各界安全领袖出席,就安全生态的共建举措达成共识:构筑无边界的安全连接;建立常态化的互联网安全合作机制;建立人才与技术的标准化是共建安全生态的三大举措。

安全生态的基础
构建无边界安全连接

在全球范围内,网络安全问题已突破传统的网络界限,且跨越了国家、地区的界限,成为泛在的全球威胁。为此,大会明确了“构建无边界的全球安全连接”,倡导建立以“开放”为起点,纵向跨越人、企业、机构、产业、政府,横向跨越企业、行业边界与国界的全连接理论。

回顾CSS安全领袖峰会的发展,从2015年BAT首次同台,到2016年国际顶级企业悉数参会,CSS平台本身就是全连接的典型示范。本届峰会齐聚全球十大科技巨头在内的500家企业,不仅在地理上跨越了国界,更在产业上覆盖了硬件制造、操作系统、安全管理平台、网络服务、互联网通信等整个安全产业链。

在CSS平台发展的同时,作为本次大会发起方的腾讯公司,也在开放、连接的实践中率先垂范。在苹果2016年WWDC开发者大会上,苹果向外界展示了针对中国用户推出的基于苹果最新移动操作系统iOS10的骚扰电话拦截功能,合作伙伴正是腾讯手机管家。此外,在微软安全响应中心公布的TOP100贡献榜中,腾讯9位安全专家入选并获致谢,成为国内获致谢最多厂商;在微软、谷歌、Adobe、苹果等国际著名厂商公布的上半年漏洞致谢公告中,腾讯也成为国内获谢最多的企业。

安全生态的保障
常态化机制保证持续生长

如果没有相应的落地机制,互联网安全的国际合作体系构建很可能会停留在纸面上。常态化协作机制成为各方一致认可的安全生态构建保障。腾讯公司副总裁马斌表示:“我们希望CSS安全领袖峰会本身不仅仅是一年一度的峰会,更是一个长效的合作平台,促进产业的常态化合作。”据悉,过去一年,CSS安全领袖峰会平台已经在互联网金融、车联网等领域举办多次交流沙龙,打破产业、企业壁垒,将交流与协作常态化。

值得一提的是,这种平台与合作机制正逐渐在行业内外落地生根。例如,除了推动CSS安全领袖峰会平台的发展,腾讯公司还赞助KEEN团队,成功举办GeekPwn黑客大赛。该赛事已成为借助白帽黑客攻防技术,关注互联网及软件厂商安全漏洞的重要平台。

腾讯更是推动中国反电信网络诈骗“警、企、民”协作模式与机制的先驱。腾讯董事会主席兼首席执行官马化腾表示,开放腾讯核心技术和数据建设反电信网络诈骗体系,是腾讯的企业社会责任。早在2013年初,腾讯公司就率先在深圳试点,推动与深圳警方、运营商,并联合100多家企业建立了反信息诈骗联盟,在打击电信网络诈骗方面取得了积极成效。2015年,腾讯安全首推“守护者计划”,推出“鹰眼”智能反电话诈骗盒子和“麒麟”伪基站实时检测系统,分别与运营商、公安部门等开展合作。腾讯守护者计划联动了腾讯公司海量大数据资源,集“犯罪打击、大数据运用、行业联合、宣传教育”四大职能于一体,开启了“腾讯模式”在各地的实践。得益于“守护者计划”这一长效合作机制,今年以来,守护者计划安全团队已协助警方破获多起特大案件,协助破获案件金额超5亿元。

安全生态的壮大
标准化的人才与技术

CSS安全领袖峰会认为:安全新生态需要无障碍的连接,而顺畅连接的前提是标准的统一,即人才与技术的标准化建设。持续的人才与技术输出将为整个安全生态输送血液和养分。

安全人才与技术的需求日益旺盛。今年7月,腾讯安全成立了国内首个互联网安全实验室矩阵腾讯安全联合实验室,旗下涵盖科恩实验室、玄武实验室、湛泸实验室、云鼎实验室、反病毒实验室、反诈骗实验室、移动安全实验室七大实验室,安全防范和保障范围覆盖了连接、系统、应用、信息、设备、云六大互联网关键领域。其中,揽获2016 Pwn2Own世界冠军的腾讯联合战队成员都参与了联合实验室的建设。

在本届峰会上,中国安全力量的发展壮大成为峰会内容之外,最为引人注目的亮点。在日益严峻的全球安全形势下,中国安全力量在推动全球建立无边界的全连接、常态化的安全合作机制、标准化的人才和技术上,正在发挥着越来越大的作用,而这一切,也将进一步促进全球安全力量的高度融合,最终形成休戚与共的安全生态体系。

腾讯副总裁丁珂:
网络安全生态核心是融合

加速构建网络安全新生态需要聚焦三个核心点:开放合作深化连接,技术创新共享成果,产业融合常态合作。

以“开放”为起点,构建纵向跨越人、企业、机构、产业、政府,横向跨越企业、行业边界与国界的全连接已经成为行业共识。惠普发布的《2015年网络安全运营状况报告》显示,全球企业在防御网络攻击方面的准备工作严重不足。在解决全球网络安全问题上,即使是全球很多顶级公司也难有万全之策。因此,全球企业和机构之间在深度和广度上的连接要全面进化,实现休戚与共的全球深度连接,这是解决全球网络问题的重要路径之一。

关于深化连接,丁珂给出了一个相对全面的解读。连接的内容包括:理念的连接,即先进安全理念的碰撞与融合;数据的连接,即安全大数据的共享;信息的连接,重大安全举措、安全威胁的互通互联;技术与知识的连接,即前沿技术的交流与合作;标准的连接,即对齐标准,扫清合作的障碍。

随着技术手段的进步,互联网安全面临更新、更棘手的挑战。各界应形成合力,在人工智能、量子通信、云安全技术等重点技术上互通有无、相互激发、加速创新、形成突破,并将这些技术能力通过合作、共享等方式快速赋予安全生态的参与者。

技术是把双刃剑,它带来进步的同时,产生的破坏力也昭然若揭。基于云技术的网络攻击、基于大数据的隐私泄露、基于智能终端的网络攻击等,已经对各行业企业的发展造成巨大威胁。如何快速利用新技术新应用,提供相匹配的网络安全解决方案,成为解决新兴网络安全的重要课题。

秉承开放、共享、融合的理念,各行业共享数据与技术,建立重大安全行动、重要威胁信息的互通互联机制。以常态机制保障产业融合的长效落地与安全生态的持续生长。同时,兼顾推动人才与技术的标准化,为跨国界、跨产业的连接、融合扫清障碍。

过去一年,CSS安全领袖峰会平台已经在互联网金融、车联网等领域举办多次交流沙龙,打破产业、企业壁垒,将交流与协作常态化。而且这种平台与合作机制也在行业内外落地生根。作为CSS安全领袖峰会的发起方、互联网安全开放生态的呼吁者和推动者,腾讯已成为最大的互联网开放平台。腾讯安全联盟成员已超百家,涵盖反诈骗、账号安全、隐私保护、支付安全、防骚扰等诸多方面,从开放合作、技术创新和产业融合三方面同时发力,为推动建立一个智慧生长的安全生态新体系做出切实的努力。