第二届网络空间安全(天津)论坛开幕

共建网络安全 共治网络空间

论坛现场 新报记者 孙震 通讯员 赵军 摄

昨日,第二届网络空间安全(天津)论坛在津开幕,该论坛是全国唯一以"网络空间安全"为主题的国际性官方论坛。

本届论坛以"共建网络安全 共治网络空间"为主题,立足最新的网络安全形势,精准聚焦大模型与数据安全制度建设、网络数据人工智能安全治理实践、智能网联汽车安全、移动互联网安全和个人信息保护、关键信息系统基础设施保护、高级威胁技术趋势等时下网络安全领域最前沿的议题,共同探讨网络空间安全领域的"硬核"新技术、未来新场景、治理新议题,有效形成网络安全治理的路径、策略、模式、标准,以系统思维推动综合治理,不断完善网络空间安全保障体系,充分引领网络安全发展新方向。

论坛整体分为论坛开幕式及主论坛,信创产业安全发展、移动应用安全生态治理、网络与数据安全法治、网络安全高级威胁防御、大模型与数据安全等5个主题论坛以及第五届国际反病毒大会和第二届"天网杯"网络安全大赛。

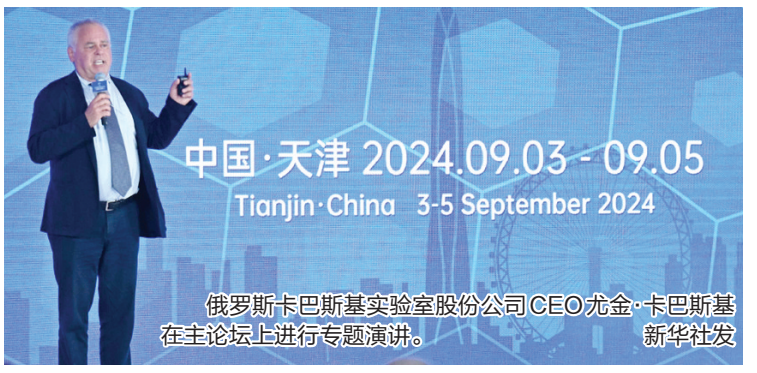
大会期间,国家计算机病毒协同分析平台正式上线,将面向国内外互联网用户和企事业单位提供数字文件安全性分析服务,有力促进全球网络安全数据共享和技术合作。国家计算机病毒应急处理中心还发布了《网络空间安全态势分析报告(2024)》《移动互联网应用安全统计分析报告(2024)》,全面梳理当前网络空间安全面临的风险挑战,从完善法律法规体系、构建共享共治格局、加快标准体系建设、健全监测预警体系等方面提出对策建议,为推进新形势下我国网络空间安全风险治理工作提供有力参考。

开幕式的颁奖仪式上,对为网络空间安全(天津)论坛作出突出贡献的个人进行了表彰。同时,揭晓了第二届"天网杯"网络安全大赛获奖名单,为18支获奖战队进行了现场颁奖。

共享理念共商对策 大咖共话网络安全

开幕式及主论坛上,近800位来自网络安全领域国际组织、部分国家执法机构、国际研究机构的负责人,中央机关、国家部委相关负责同志,两院院士、知名专家学者和科研院所、金融机构、国内外知名企业、高校代表齐聚一堂,共话网络空间安全形势、共享网络安全理念、共商网络安全对策。

中国工程院院士邬江兴、中国科学院院士郑建华、国际刑警组织网络犯罪局副局长董健、俄罗斯卡巴斯基实验室股份公司CEO尤金·卡巴斯基、360集团创始人周鸿祎、奇安信科技集团董事长齐向东分别围绕《内生安全理论方法赋能数字产业新质生产力》《密码定义安全——思考与愿景》《国际刑警组织打击网络犯罪战略和主要举措》《网络时代的网络免疫》《打造安全大模型,用AI重塑安全》《保障"数据三角"安全:新时代网络空间安全的首要任务》等作了专题报告和精彩演讲。



俄罗斯卡巴斯基实验室股份公司CEO尤金·卡巴斯基在主论坛上进行专题演讲。 新华社发

邬江兴院士在报告中提到,人类社会正在迈向以数据为关键的数字经济时代,其中网络安全问题愈加复杂。现行网络安全方法陷入不断打补丁的恶性循环,难以应对多重安全挑战。部分专家学者提出数字生态系统底层驱动范式转型,期望将使用安全向设计安全转型来解决安全问题,但是其仍未跳出传统网络安全困境。通过对网络空间安全第一性问题再认知——存储程序控制构造基因缺陷,基于内生安全理论方法进行网络弹性设计来解决网络安全问题。通过动态异构冗余构造(DHR)在不确定安全问题空间创建基于可控概率的安全可信服务环境。实践证明内生安全赋能的网络弹性设计能够从根本上解决不确定安全威胁,实现可量化设计和验证的安全优化。

"密码定义安全,是要尽可能将安全与密码绑定。"郑建华院士表示,基于可证明安全的思想,将密码技术作用在保护对象上,将信息系统中的重要安全问题归约到密码系统的安全上。网络安全的本质是对抗,在此范式下,网络攻击能否得手仅取决于敌手能否突破密码防护,顺理成章地将网络安全的攻防"规约"为密码的攻防。主要包括密码定义数据安全、密码定义网络安全和网络计算安全。

董健表示,长期以来,国际刑警组织与全球各国执法机构、网络安全机构和网络安全企业以及各利益相关方共同协作,共同打击网络犯罪。他呼吁国际刑警组织各成员国、各利益相关方,共同加强打击网络犯罪领域的合作,加强打击网络犯罪相关的信息共享,更加有效地利用国际刑警组织的渠道和平台,共同打击网络犯罪,保护全球网络空间安全和社区安全。

卡巴斯基认为,当前网络安全面临三大问题,首先是网络犯罪规模快速扩张,其次是犯罪团伙日趋专业化且攻击针对性越来越强,三是网络攻击目标逐渐转向工业系统和关键基础设施。对此,在执法、教育和技术三方面进行深入合作,是保护网络空间安全的关键因素,尤其是国际执法机构之间的合作至关重要。

"必须要用AI应对AI攻击",周鸿祎在演讲中讲道,当前AI技术深刻影响各行各业,在为新质生产力发展带来机遇的同时,也带来诸多全新安全挑战,必须用AI重塑安全,依托专业化大模型方法论,打造安全大模型,重塑安全产品,引领安全行业革命。

齐向东认为,数据安全占据网络空间安全的核心位置,保障数据安全的核心是保障由生产域、应用域、流通域组成的"数据三角"安全。其双向连通性决定了其中一个域出现安全问题,就会影响全域。目前,"数据三角"各自孤立地建设安全防护系统,是数据安全的最大漏洞,加快推进体系化的网络和数据安全建设,成为筑牢新时代网络空间安全防线的唯一出路。

本组撰文 新报记者 张艳

违规收集个人信息比去年同期有下降

昨日,第二届网络空间安全(天津)论坛在天津开幕。论坛上,由国家计算机病毒应急处理中心发布的《移动互联网应用安全统计分析报告(2024)》显示,对比去年同期抽样检测的应用,应用存在侵犯用户权益的现象有所下降,其中"违规收集个人信息"违规类型占比从去年的29.54%下降至今年的15.09%,占比降幅较大。

国家计算机病毒应急处理中心对全国近一年更新、发布且下载量靠前的应用进行了个人信息合规性自动化抽样检测,共抽检15万余款App应用,发现超32.82%的移动互联网应用存在侵犯用户权益的现象。

其中,存在"超范围收集个人信息"的占比27.11%;存在"App频繁自启动和关联启动"的占比19.51%;存在"违规收集个人信息"的占比为15.09%。对比去年同期抽样检测的应用,"违规收集个人信息"违规类型占比降幅较大。

国家计算机病毒应急处理中心专家刘彦表示,这一变化与监管机构加强监管息息相关。随着《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等多部相关法律和规定的落地,个人信息保护的法律法规体系日趋完善,使得移动应用在收集、使用个人信息时有了明确的规范。

各开发企业、运营企业也加强了这类个人信息违规应用的安全风险监控,应用商店也在上架审核阶段把控更为严格,随着相关安全检测技术能力的提升,提前发现问题的几率增加,存在这类问题的应用相应也减少较多。

据新华社电

信息缺失问题好转 近半App有责任人

国家计算机病毒应急处理中心抽样25万个App进行统计分析,发现截至今年6月,49.17%的App有明确开发/运营主体。这是从昨日召开的第二届网络空间安全(天津)论坛上获悉的。

由国家计算机病毒应急处理中心在论坛发布的《移动互联网应用安全统计分析报告(2024)》指出,抽样结果较去年同期增长10.32个百分点。国家计算机病毒应急处理中心专家刘彦表示,这说明我国移动互联网应用责任主体信息缺失问题有所好转。

去年7月,工信部发布《工业和信息化部关于开展移动互联网应用程序备案工作的通知》,并给出备案路线图,明确2023年9月至2024年3月为存量App备案阶段。

2022年6月,国家互联网信息办公室发布新修订的《移动互联网应用程序信息服务管理规定》,对应用程序分发平台制定了明确的规定和要求,要求应用程序分发平台对存在数据安全风险隐患,违法违规收集使用个人信息的,不得为其提供服务。截至今年6月,国家计算机病毒应急处理中心对移动互联网应用分发渠道进行监测,发现存在Android恶意程序的数量相比去年同期增长明显。

报告指出,分发渠道长期存在恶意程序和违法移动互联网应用,主管部门和监管部门对分发渠道管理力度需要加强。

据新华社电