网安周主论坛多位行业大咖、专家学者共论如何筑牢网络安全防线

深化大湾区网络安全合作 从被动响应转为主动防御

9月9日,2024年国家网络安全宣传周网络安全技术高峰主论坛暨粤港澳大湾区网络安全大会在广州南沙举行。来自政府部门、通信行业有关负责人、专家院士和企业负责人作主旨演讲,分享如何共同筑牢网络安全防线、携手推进数字经济高质量发展的真知灼见。同时,主论坛上,全国网络安全标准化技术委员会(以下简称"网安标委")发布了《人工智能安全治理框架》1.0版。

■采写:新快报记者 黄闻禹 陈慕媛
■摄影:新快报记者 毕志毅

■9月9日,2024年国家网络安全技术高峰主论坛在广州南沙举行。

1 关键词 协同防护

加大安全协同 共建网络协同防御体系

香港数字政策办公室数字政策专员黄志光分享了香港特区政府在网络安全方面采取的最新策略与发展保障方式。他介绍道,香港特区政府在网络安全方面的目标主要有以下三项:首先,为香港的数字化发展提供一个安全稳妥的网络环境,维护数据自由流动的灵活和开放环境;其次,确保政府的信息技术基础设施、系统与信息安全可靠;第三,提高公众及企业对网络安全的认知。

黄志光表示,为了应对与日俱增的网络安全威胁,香港特区政府于今年7月份成立了数字政策办公室,加快推动数据政府建设,提升数据治理能力,全力推动数字经济发展。"其中一个重要职能正是加强政府内外系统和数据的保护,为香港特区政府的数字化转型和发展数字经济提供坚实基础。"

黄志光表示,香港将继续努力构建安全稳定的网络环境,增强和提升业界和公众的网络安全意识与应变能力,融入粤港澳大湾区的发展,推动与健全香港国际创新科技中心建设。

"网络安全关乎国家安全体系的方方面面,没有网络安全就没有国家安全。"来自澳门网络安全事故预警及应急中心主管何永坚同样介绍了澳门在网络安全保障方面的应对策略。他指出,澳门每年都有政府部门或重要机构遭受网络攻击,幸好澳门有一套比较完善的管理体系、应急预案,可以及时修复受影响的网络服务。

"网络安全是共同的,不是孤立的。"何永坚期待,要深化粤港澳大湾区网络安全的合作,包括加强网络安全信息共享,协同应对重大网安事件,以及促进人才培养和技术创新。

"我26年前来到了大湾区,在这里开始第一份工作,再到安家与创立公司。这一路走来,见证了大湾区澎湃的经济活力和持续的创新动力。"作为来自行业企业的代表,深信服科技有限公司董事长何朝曦认为,作为大湾区面向国际的窗口,香港和澳门发挥着重要作用,但也面临着越来越多的网络安全风险与挑战。

"尤其是随着新技术发展,新型的网络攻击层出不穷,攻击的成本越来越低。"何朝曦说,随着市场的拓展,越来越多的企业走出国门、走向世界,面对的网络安全风险也越来越复杂,而目前大部分企业、网络用户仍存在重建设、轻运营与轻防护的现象。

如何应对新的网络安全挑战?何朝曦给出的答案是协同。"只有加大内地和港澳的安全协同,才能保障好大湾区数字经济的发展。"他认为协同的关键在于统筹机制,有关部门需要在大湾区建立一个在国家统一领导下的协同防御体系,融合各方力量,高效协作抵御网络攻击。

"在多方协同和不断努力下,大湾区将打造成全球网络安全产业的创新聚集地,中国的网络安全产品和技术,才能够更好地从服务湾区走向服务全球。"他补充说。

2 关键词 护卫体系 从"端边网疆"构建国家网络安全防御体系

中国工程院院士方滨兴就《积极打造网络安全护卫体系》题目进行发言。首先,他从安全模式、内涵、政府的作用、典型方法等多个层面重点分析阐述了网络安全护卫中的自卫模式与护卫模式的区别。

"就像驱蚊灯的普适性,在于其驱蚊机理仅与蚊虫有关,与人的身体素质无关。这就是解耦的效果。"方滨兴表示,护卫模式属于外置安全防御,这是一种与应用系统细节无关(解耦)、只关注攻击者是谁的防御模式,具有普适保护能力;而自卫模式属于内生安全防御,是利用应用系统自身的能力来进行安全防御而不关心攻击者是谁的防御模式。

"自卫模式与护卫模式的典型方法分别是拟态防御和盾立方。"基于两种不同防护方式的表现和作用,方滨兴提出打造"盾立方"护卫模式,这是一套以威胁情报分析与反制中心(CTIC)为核心的联动式协防体系,通过感知、研判、阻断之间的协同联动,形成一种基于"护卫模式"的信息系统保障体系。

他进一步指出,"盾立方"将防御重心从"关注保护对象自身安全"转变为"关注发现和阻断攻击者",支撑了护卫模式的理念。尤其是通过"阻断",让网络安全防御回归本质,即拦截与清扫,而不仅仅是补漏洞。方滨兴认为,国家需要构建有组织的护卫模式,归纳起来是"端边网疆"纵深防御体系。"端"是端防,即用户自卫;"边"是企防、城防,"盾立方"可以作为企防与城防的手段;"网"是运营商网防;"疆"是国家做一个网络疆界,拦截境外网络攻击。

3 关键词 防御体系 网络安全应从被动响应转向主动防御

杭州安恒信息技术股份有限公司董事长范渊对在线应用安全、数据库安全和审计有极其深入研究,他认为,网络安全的攻防,始终处于一个非对称的状态,或者说非公平的状态。他分享了自己多年来的思考、观察和实践,"对于攻击方来讲,它只需要做单点的突破,甚至游击战,就可以达到很好的效果。而每一个防御单位必须构建起无懈可击的防御堡垒。"

他表示,近年来网络攻击者攻击手段不断自动化、智能化,攻击的效果不断提升,而防御方大多停留在被动监测响应的阶段。尽管在被动防御的资源投入上一直在增加,但面对网络威胁的应对与建设效益正在减弱。

对此,他建议网络安全防护需要的不仅仅是修补漏洞,更需要一种全新的思维和方法,包括思维、技术和体系的三重升级。思维更新,人们要从短期见效的目标转变为注重长期的战略,将威胁跟踪作为常态化长期化的工作;技术升级,体现为从被动响应转变为主动追踪。体系打造,防御方要从单打独斗转变为协同防御。

通信与金融行业作为网络安全的重点领域,网络信息安全尤为重要。"随着网络安全的内涵不断丰富,外延不断扩大,迫切需要建立国家级协同防御体系。"中国联合网络通信集团有限公司董事长、党组书记陈忠岳也认为,为应对来自网络的不确定性威胁,网络安全工作应实现防御工作从被动到主动,从静态到动态,从单点到整体的技能升级。

陈忠岳介绍,中国联通体系化构建网络安全基础设施,强化核心机房、核心网络、关键路由、关键系统的安全,打造实战化、集约化、智能化的网络安全防御体系,坚决保障通信畅通与安全。中国联通还在广州支撑建设了国内首个超大城市数字安全运营中心,实现数字安全基础设施一体化、运营管理一体化、联防联控一体化,助力打造护航数字政府建设的广州样板。

"当前信息技术与金融业务深度融合发展,也带来了日益严峻复杂的网络风险。"中国人民银行科技司司长李伟谈道,在金融网络安全防护体系当中,金融业关键信息基础设施是重中之重。

他表示,金融网络是由庞大复杂、多种多样的软硬件设备构成的,涉及的专业多,运维的难度大,可靠的产品和服务供应链也是保障网络安全的重要一环。因此,协同防御是金融网络安全的必然选择、现实选择。"中国人民银行愿与各方共同努力,加强网络风险协同监测,强化网络安全信息共享,开展平台对接联合研判协同处置,探索跨行业应急演练,携手筑牢金融网络安全整体防线。"

新闻延伸 《人工智能安全治理框架》1.0版发布

9月9日,全国网络安全标准化技术委员会制定的《人工智能安全治理框架》1.0版(以下简称"《框架》"),对外公开发布。

《框架》以鼓励人工智能创新发展为第一要务,以有效防范化解人工智能安全风险为出发点和落脚点,提出了包容审慎、确保安全,风险导向、敏捷治理,技管结合、协同应对,开放合作、共治共享等人工智能安全治理的原则。

《框架》按照风险管理的理念,紧密结合人工智能技术特性,分析人工智能风险来源和表现形式,针对模型算法安全、数据安全和系统安全等内生安全风险和网络域、现实域、认知域、伦理域等应用安全风险,提出相应技术应对和综合防治措施,以及人工智能安全开发应用指引。

网安标委秘书处主要负责人表示,《框架》1.0版的发布,对推动社会各方积极参与、协同推进人工智能安全治理具有重要促进作用。同时,也有助于在全球范围推动人工智能安全治理国际合作,推动形成具有广泛共识的全球人工智能治理体系,确保人工智能技术造福于人类。