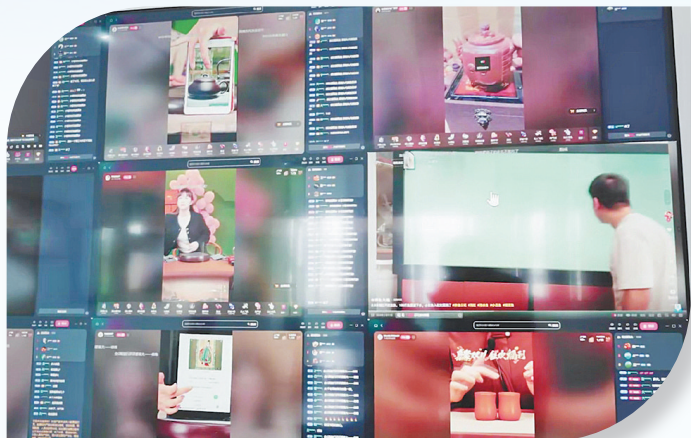


警务联络官

数盾护航 智安未来

从宜兴紫砂壶里的文化IP守护,到锡山电动车车间的数据资产保卫,无锡公安网安警务联络官化身企业身边的“数字医生”,以“无事不扰、有事必应”的承诺,将警务服务延伸至网络空间最前沿,为地方特色产业筑起一道坚不可摧的“数字防线”。



全链打击 擦亮“紫砂”金字招牌

“这批‘大师壶’在直播间卖得正火,可咱们企业的订单却少了三成。”今年初,宜兴市公安局网安警务联络官在走访某头部紫砂企业时,听到了企业负责人满腹的委屈。直播间里,“假大师”声情并茂,“假证书”精美绝伦,而真正的匠心之作却无人问津,“劣币驱逐良币”的困境让宜兴紫砂

的文化IP形象受损。

面对企业的急难愁盼,网安警务联络官没有停留在倾听层面,而是敏锐捕捉到这一行业痛点,迅速启动协同响应机制。警方依托大数据技术,对涉案直播间进行全量数据梳理,精准锁定多个长期从事违法销售活动的直播间。民警深入剖析直播运营模式,

式,固定主播虚假宣传、雇佣“托儿”虚假消费等电子证据;同时向线下延伸,彻查制壶、刻绘、仓储物流等全链条环节。

随后,警方收网,抓获涉案人员百余人,查封制假窝点、仓库及直播间多处,扣押假冒名人紫砂茶壶万余把、疑似假冒大师证书的字画数千张,涉

案价值巨大。在案件侦办过程中,警方还主动牵头检察院、法院、市监部门及行业专家召开专题座谈会,解决行为定性和真伪鉴定难题,凝聚执法共识。这一行动有力打击了紫砂行业制假售假违法犯罪行为,切实维护了产业品牌声誉,让“宜兴紫砂”的金字招牌在网络安全屏障下熠熠生辉。

法规引领 筑牢安全“防火墙”

“现在法律处罚力度这么大,企业如果连基础网络安全管理都没做好,风险实在太大了。”近日,梁溪区文旅集团的一间会议室里气氛热烈。梁溪公安分局网安警务联络官正站在讲台前,结合最新修订的《中华人民共和国网络安全法》,为集团员工讲授一堂兼具实战性与法规性的“网络安全课”。

这场培训并非例行公事,而是梁溪网安针对辖区文旅、商贸等重点行

业企业推出的“合规护航”专项行动。培训伊始,联络官并未直接罗列法条,而是抛出了一个令人揪心的案例:“近期多起木马攻击事件中,不法分子伪装成客户发送文件,受害者往往因为一时疏忽,导致核心账户信息泄露。很多时候,不是技术不够强,而是安全意识这道‘安全阀’没拧紧。”

现场,一名年轻员工忍不住发问:“我们平时觉得防病毒软件开着

就没事,这种社会工程学攻击怎么防?”联络官借此深入剖析作案手法,提醒大家面对来历不明的文件与链接时务必多留心眼,从源头阻断风险。随后,话题转向新修订的《网络安全法》。联络官严肃指出,新法大幅提高了违法处罚上限,并新增了人工智能安全条款。“这不仅是对法律红线的提升,更是对企业全面梳理网站及App备案情况,明确

负责人,要切实扛起网络安全“大旗”。

从“被动应对”到“主动预防”,梁溪网安通过常态化、精准化的人企服务,将专业防护力量延伸至基层末梢。这种“送法人企、送技入企”的模式,不仅帮助企业拧紧网络“安全阀”,更让“企业安全就是生命线”的理念真正落地生根,为无锡经济社会高质量发展营造安全稳定的网络环境。



精准护航 斩断伸向数据资产“黑手”

“李厂长,你们这条生产线昨晚有过三次异常外部访问,虽然没造成损失,但这是个危险信号。”锡山公安分局网安警务联络官指着屏幕上的日志,向某电动车制造企业负责人指出隐患。面对这一“沉睡”的风险,联络官变“坐等报案”为“主动出

击”,深入企业一线开展“一对一”网络安全体检。

针对传统制造企业在网络安全防护上技术薄弱、意识不足等痛点,联络官不仅提供法律咨询,更送上定制化技术指导。今年以来,已累计向多家电动车制造企业通

报涉及多个系统的潜在安全漏洞,督促限期整改。前不久,在侦办一起仿冒网站案件时,联络官在走访中敏锐发现辖区多家制造企业存在异常访问及数据传输日志,循线追踪后在企业终端电脑中查获“木马”样本,成功完善证

据链,斩断了伸向企业数据资产的“黑手”。

锡山公安通过以案释法发布预警,进一步提升了企业辨识仿冒软件、木马病毒的能力,让互联网更好地赋能地方经济发展,为传统制造业筑牢了“防火墙”。

技术溯源 破解企业“数据焦虑”

“章警官,上次整改后,我心里一直不踏实,怕隐患没除根。”今年8月,惠山区一家重点制造企业的负责人在与网安警务联络官沟通时,吐露了这份“数据焦虑”。

惠山公安分局网安大队没有止步于常规的指令性处置,而是将关口前移,组建专家团队上门开展全方位的“网络安全体检”。“体检”的核心在于全量数据回溯与深层漏洞诊断。民

警依托专业工具,对企业历史流量进行深度挖掘,重点对前期整改情况进行“回头看”。通过比对整改后的流量特征,核实确认涉事设备已离线、恶意通信行为已彻底终止,用数据验证了整改的实效性,让企业吃下“定心丸”。

更为关键的是,检查人员敏锐发现了企业办公Wi-Fi长期存在的重大配置缺陷,这一漏洞如同悬在企业头顶的“定时炸弹”——员工私带设

备接入内网后,一旦感染病毒,不仅易造成横向传播,更因缺乏实名绑定而难以追溯责任人,隐蔽性极强。

发现问题只是第一步,如何根治才是关键。惠山网安坚持“查病必除根”,在技术层面建立全维度安全画像,确保处置有据可依;在治理层面,指导企业限期部署网络准入控制系统,从源头切断恶意代码传播链。

这种“技术手段硬约束”与“管理

制度软约束”的双轮驱动,实现了真正的闭环治理。目前,该企业已建立严格的终端接入认证体系,实现了“人、机、网”的实名绑定与可视可控。

从“被动处置”到“主动体检”,从“单点救火”到“系统防火”,惠山网安以个案服务推动行业治理,帮助科技企业实现了从“被动防御”向“主动免疫”的跨越,为辖区重点企业数字化转型筑牢了坚实的安全屏障。



分级监管 拧紧产业“安全阀”

“警察同志,我们的后台突然提示服务器被攻击,核心数据面临泄露风险,这可怎么办?”今年6月的一天,滨湖公安分局网安警务联络官的手机骤然响起,辖区一家重点电商企业的负责人声音急切。网络安全事件突发性强、危害大,稍一疏忽就可能造成不可挽回的损失。依托警务联络官机制建成的7×24小时应急响应

体系,联络官立即启动绿色通道,一边远程指导企业技术团队切断受感染节点的网络连接,阻断攻击路径;一边迅速协调专业力量,指导企业清除病毒、修复系统。在警企高效联动下,一场潜在的数据泄露危机被控制在萌芽状态,最大限度降低了经济损失。

滨湖网安并未止步于“救火”,而是坚持“处置一案、排查一片、治理一

类”的工作理念,在平息突发警情的同时,联络官带领技术骨干对企业开展了深入的“网络安全体检”。通过全面排查网络架构、账号权限、数据存储等关键环节,建立隐患台账,逐项落实整改,将风险隐患消除在萌芽状态。

“过去我们总觉得安全是技术部门的事,出了事再找警察。现在才明白,预防管理也是‘生命线’。”该企业

的信息安全负责人表示。

滨湖公安坚持“服务与监管并重”,针对辖区行业业态差异,紧盯新增备案网站、重要业务系统等重点网络资产,实施分级分类监管。此外,围绕勒索病毒防范、重要数据备份等高频风险点,联络官还开展靶向式安全培训,推动企业网络安全由“被动应对”向“主动防范”转变。



科技赋能 当好科创“数字扫雷手”

“扫描设备一开,我们整个产线都要停摆,测试数据全得重来,这风险谁担得起?”今年5月中旬,新吴公安分局网安警务联络官走访一家重点软件企业时,听到了技术人员的顾虑。该企业长期面临网络防护漏洞难以根治、症结不清的困扰,但出于

对生产稳定性的担忧,始终无法配合深度排查。

针对这一痛点,联络官并未止步于口头建议,而是迅速对接上级部门资源,引入专业“扫雷”设备进驻部署。面对企业担心扫描占用带宽、影响正常业务测试等实际困难,联络官

采取“错峰扫描、逐节点摸排”的策略:利用夜间低峰期进行深度扫描,白天仅做轻量级监测,既保障了企业网络带宽的正常需求,又确保了排查无死角。经过多轮调试与协调,最终顺利完成了全网扫描部署,成功将核心数据隐患消灭在萌芽状态。

通过主动靠前服务、引入专业技术手段、建立快速响应机制,新吴公安有效帮助科技企业解决了自身难以发现的技术盲区,以“主动一步”换取企业“安心一分”,为无锡高新区科创发展营造了安全稳定的网络环境。(网安)